AFMC THE ASSOCIATION OF FACULTIES OF MEDICINE OF CANADA

Request for Proposals

Database Development Services

Submission Deadline: Friday, June 30, 2023, at 5pm (EST)

Background

The National Consortium for Indigenous Medical Education (NCIME) is a partnership between the Indigenous Physicians Association of Canada, the Association of Faculties of Medicine of Canada, the College of Family Physicians of Canada, the Medical Council of Canada and the Royal College of Physicians and Surgeons of Canada. The NCIME was formed to implement Indigenous-led work streams that will transform Indigenous medical education and contribute to the delivery of culturally safe care.

The NCIME has established six working groups focused on making improvements in priority action areas. The six working groups are chaired by members of the NCIME Executive Committee and include an Associate Chair who is a resident or early-career physician and an Elder or Knowledge Keeper. The NCIME staff provides administrative, research and evaluation support and consultants are utilized as needed for special areas of expertise.

The NCIME Working Groups will provide leadership and support to partners to address areas of common priority as they fulfil their collective responsibilities. The working groups will transform Indigenous medical education and contribute to the delivery of culturally safe health care. Each working group is led by an NCIME Executive Committee member, aligning areas of expertise with the six priority areas:

Assessment of Indigenous Studies, Cultural Safety and Anti-Racism

- Guidelines for the development of assessment tools including OSCE (objective, structure, clinical exam) and MMI (maximum medical improvement) stations, MCQ (multiple choice questions), SAMP (short answer management problems) and in-practice assessments.
- Development of some sample tools (assessment items) including quality improvement and evaluation

Indigenous Student Admissions and Transitions

Work with the 17 schools of medicine to set school-specific minimum number of First Nations, Métis and Inuit students for admission each year.
Develop guidelines for admissions/transition processes and assessment criteria, applicable across the continuum, for all candidates to medical school that assess knowledge of Indigenous studies, cultural safety and anti-racism.
Collaborate with all 17 schools of medicine to define and ensure robust data collection and reporting annually that allow for review of progress toward goals at the individual school, provincial and national level.

Anti-Racism

- Identify the core elements of anti-racism policies and processes.
- Develop a learning module to support the implementation of anti-racism policies and processes.

- Increasing admissions / transitions of Indigenous students across entry points during medical education and developing accountable admissions processes (undergraduate medical education / post-graduate medical education / transition to practice)
- Work with the 17 schools of medicine to set school-specific minimum number of First Nations, Métis, and Inuit students for admission each year.
- Develop guidelines for admissions/transition processes and assessment criteria, applicable across the continuum, for all candidates to medical school that assess knowledge of Indigenous studies, cultural safety, and anti-racism.
- Collaborate with all 17 schools of medicine to define and ensure robust data collection and reporting annually that allow for review of progress toward goals at the individual school, provincial and national level.

Indigenous Faculty Recruitment and Retention

- Develop and maintain a database of Indigenous physicians and health professionals/ educators who are interested in contributing to Indigenous Medical Education
- Create and implement a leadership development program for Indigenous Medical Educators
- Collaborate with the 17 schools of medicine to create short- and long-term plans to support the attainment of critical masses of Indigenous Faculty
- Develop a plan to identify and foster leadership development in Indigenous medical learners starting at the time of admission.

Improving Cultural Safety in Curriculum

- Ensuring that the curriculum frameworks and graduating outcomes / competencies from each build on each other with cultural safety and anti-racism / anti-colonialism as core pedagogical approaches
- Identifying the faculty development needs to support the implementation of longitudinal Indigenous health curriculum.

Indigenous Physician Wellness and Joy in Work

- Develop a framework that defines wellness and joy in work for Indigenous physicians.
- Support the implementation of the frameworks by IPAC, the organizations, and the 17 schools of medicine.
- This project emphasizes use of formative and summative evaluation and impact assessment through standard metrics as well as utilizing Indigenous approaches and evaluation frameworks.

Instructions to Vendors

1. Requests for Information

Vendors are solely responsible for ensuring that they have obtained all information necessary to prepare their proposal and for independently verifying such information. Although all reasonable efforts have been made, the NCIME does not warrant that any information provided is accurate, complete, reliable or sufficient. Vendors shall be deemed to have gathered all information necessary to perform their obligations under the RFP.

Vendors are expected to inform themselves with respect to all terms or conditions that may affect this proposal, and to ensure that they comply.

Vendors who find discrepancies or omissions in the information provided, or who have questions as to the meaning or intent of various aspects of the project, shall at once, notify the NCIME contact(s) identified in the RFP, who will, if necessary, provide written instructions, clarifications, or explanations.

Unless confirmed in writing by NCIME contacts or issued by addendum on the NCIME's website, vendors shall not take into consideration any verbal instructions, comments or answers to questions which purport to modify the RFP document.

All inquiries related to this RFP shall be submitted in writing, by email, to NCIME contacts.

2. Negotiation with Vendors

The solicitation of proposals does not in any way commit the NCIME to accept any proposal or to commence negotiations with any vendor.

Following the evaluation of the submitted proposals, the NCIME will consider entering into negotiations for a contract with any of the vendors it believes best meet the needs and expectations of the organization and offers the best overall content and value.

The NCIME reserves the right to negotiate with any or all of the vendors, including those vendors who have submitted a proposal that does not fully comply, either in material or non-material ways, with these RFP requirements.

2.1 Proposal Costs to Vendor Account

All costs required to complete the proposal of whatsoever nature, including but not limited to documents, reproduction, travel, meetings and toll calls, are the sole responsibility of the vendor.

2.2 Implied Acceptance of Terms and Conditions

By submitting a proposal, the vendor agrees to abide by the terms and conditions outlined in this RFP.

2.3 Separate Submissions for Technical and Costs

Vendors must submit their proposals via email in two separate and distinct PDF electronic documents. One electronic document to be marked "Technical" must contain details of the proposed solution, services, and approach (ex. no cost information or reference thereto) and the second electronic document to be marked **"**Financial**"** must contain only cost information (ex. cost estimation model).

Scope of Work

The NCIME is seeking solutions for:

1) Setting up Microsoft 365, applying for Microsoft's Nonprofit status, consolidating cloud-based applications, and completing data migration from our current multi-repository set up. The NCIME is currently sharing a Microsoft 365 tenant maintained by the AFMC.
2) Ensuring that all content is secure using Microsoft 365 Defender and aligning policies with the NCIME's security objectives.
3) A registry, including associated systems and managed services.
4) Learning management system capability

Overview

An integrated solution is desired to achieve the main priorities of independent IT platform to control the NCIME's policies, procedures and configuration, centralized document management and communication tools, and improving use of technology and security for better content and user management. Capabilities include:

- Use Microsoft 365 as sole platform to replace multiple applications.
    - MSP will configure to meet the NCIME's needs and follow industry best practices.
- Wherever possible, replace local applications with cloud-based applications.
- User authentication with Azure AD
    - Includes external collaborators who will need access to files.
- Mailbox migration from the AFMC tenant to the NCIME tenant
- User training for the NCIME team and external collaborators

An integrated solution for the registry is desired with capabilities include:

- Dynamic, easy-to-use portal for data entry; a public-facing website; a customer relationship management system (CRM)
- Vendors will be expected to provide some form of master data management (MDM) or equivalent as part of an enterprise-wide data management solution; an optimized, flexible and efficient data architecture.
- The solution will preferably be cloud-based, commercial off-the-shelf (COTS), and must reside in a secure Canadian data centre.
- NCIME's new website must provide easy navigation for users across a variety of devices, platforms, operating systems and browsers to retrieve information and services.
- The successful vendor(s) must describe how they would satisfy NCIME's requirements in a timely, cost effective, expert phased approach.
- They must also be prepared to approach their proposal and the work in a collaborative, transparent manner, sharing with NCIME the details of their planning, costing, scheduling, billing, logistics and execution in an effort to provide the most open, smoothest, least disruptive transition possible.

Current State Assessment

- The NCIME has seven (7) employees and approximately 60 external working group members. It has one English and one French domain, ncime.ca and cnfmsa.ca. The NCIME currently shares M365 tenant with and receives all Information Technology (IT) support from the AFMC. The current licensing for the NCIME users is Microsoft 365 Business Premium (Nonprofit Staff Pricing).
- Current challenges include limited control over IT implementation and management, no centralized workspace to optimize communication and collaboration, and information security concerns around the use of personal accounts.
- A third-party external review of the NCIME IT systems was completed and found the following issues:

- M365 Hybrid identities using Azure AD Sync single sign-on, external users are added as identities, multiple cloud products = multiple accounts, the NCIME has little to no control on the M365 platform configuration and there is no dedicated IT team.
- The review also found that our software is not cloud-aware. Current issues are no centralized information management repository, limited integration between applications, no centralized security and limited auditing capacity.
- Issues with file management are fragmentation of critical information, information findability, version control problems and significant duplication of content.
- Data and account security has an increased risk of compromised security due to security being managed locally on the computer. The NCIME also has more security to manage currently due to multiple cloud environments. There is no security for external stakeholders as it is not possible to secure Gmail, Hotmail, and other personal accounts. The NCIME needs to centralize security management.

Project Management & Cost Estimation Information

As an approach to minimizing project implementation risks, improving the accuracy of work estimates. and minimizing overall costs, the NCIME intends to work in partnership with the successful vendor to confirm project scope, milestones / work packages, resource requirements and cost estimates.

Therefore, vendors should submit a sample of their cost estimation model used to calculate project. effort, timelines, and cost estimates as part of their proposal. If a recognized formal cost estimation model is used (either paper-based or software) it should be specifically referenced.

Some finalization / clarification of financial estimates, milestones and work packages may occur prior to signing any contract; however, the majority of such effort is anticipated to occur on a continuing basis, throughout the contract and project life.

Deliverables

1. Phase 1: M365 Set-Up

The objective of Phase 1 is for the NCIME to gain IT independence and the following steps will be followed:

1. Licensing will be not-for-profit M365 E3.
2. The MSP will configure to meet the NCIME's needs and follow industry best practices.
3. The MSP will provide access to all M365 applications:
    a. Office – Excel, Forms, Outlook, PowerPoint & Word
    b. SharePoint
    c. Teams
    d. OneDrive
    e. OneNote
    f. Exchange
    g. Planner
4. The MSP will migrate the NCIME mailboxes from the AFMC tenant to the NCIME tenant.

The desired timeline to complete this phase is on or before August 31, 2023.

1.1 Phase 2: SharePoint and Teams

The objective of Phase 2 is to improve collaboration and communication among the NCIME team and our external stakeholders, the following steps will be followed:

1. Information Architecture:
    a. The MSP will work with a designated NCIME team member to define how information will be organized and classified to improve how users get work done.
    b. The MSP will work with a designated NCIME team member to define the SharePoint and Teams structure for its groups.
2. Collaboration Configuration:
    a. The MSP will configure SharePoint and Teams to meet the NCIME's requirements.
3. Content Migration:
    a. The MSP will work with a designated NCIME team member to identify content on workstations, Box, Google Drive and move it to the appropriate SharePoint locations.
4. User Training:
    a. The NCIME's users and external collaborators will receive training for SharePoint, Adobe, OneDrive, Teams and Planner as they relate to the NCIME processes.
    b. Super user training will be required for designated NCIME team members in order to manage settings and permissions for the different M365 applications.

The desired timeline to complete this phase is on or before September 31, 2023.

1.2 Phase 3: Securing Content

The objective of Phase 3 is to protect the NCIME information assets, to do so, the following steps will be followed:

1. Multifactor Authentication (MFA) and Access Policies:
    a. The MSP will tailor policies to align with the NCIME's security objectives and Microsoft best practices.
2. M365 Defender:
    a. The MSP will tailor policies to align with the NCIME's security objectives.
3. Sensitivity Labels:
    a. The MSP will work with a designated NCIME team member to define and configure sensitivity labels in M365 (Public, General, Confidential, Highly Confidential).
    b. Each sensitivity label is to have its own behaviour to ensure documents are properly secured.
4. Data Loss Prevention:
    a. The MSP will work with a designated NCIME team member to define how information needs to be secured.
    b. The MSP will configure security based on the definitions made with the NCIME.

The desired timeline to complete this phase is on or before November 30, 2023.

1.3 Phase 4: Cloud-based Application Consolidation

The objectives of Phase 4 are to streamline software management and licensing, to increase application integration, and improve collaboration. The following steps will be followed:

1. Identify Applications:
    a. The NCIME has identified the following applications, which we would like to consolidate as much as possible:
        i. SharePoint
        ii. OneDrive

iii. Adobe Cloud add-on
iv. Teams
v. Exchange
vi. Planner – *Important Note: migration will need to be completed from MS Project where our current Team Workplan is housed.*
vii. Research Software compliant (SPSS, NVivo, Strata, Otter.ai)
viii. Power Pages
ix. Dataverse

b. The MSP will work with a designated NCIME team member to complete an in-depth review of the current use of applications and confirm the functionality available in a suggested replacement.
c. The MSP will work with a designated NCIME team member to prioritize the order of transition.

2. Pilot Implementations:
   a. The MSP will work with a designated NCIME team member to configure each M365 app and conduct a short pilot to test the functionality and features of all suggested replacements.
3. Rollout and Training:
   a. Selected M365 apps will be rolled out to all NCIME users and external collaborators.
   b. The MSP will work with a designated NCIME team member on a training approach for each application.

The desired timeline to complete this phase is on or before March 31, 2024.

1.4 Solution Components – The Registry & Associated Integrated Application Environment

The NCIME requires an integrated, highly configurable, and scalable solution with open APIs. Such a solution must provide for:

- Registry system (integrated application environment & a public-facing website, including a content management system)
- Learning management system
- Dynamic, easy-to-use portal for data entry
- Customer relationship management system (CRM)
- Data call programs
- Ability to perform analytics on migrated historic data.
- Case management system
- Enterprise content management system
- Automated accounting, billing, costing, and pricing functionality.
- Versatile, self-service descriptive and predictive analytics capability
- Enterprise data management system
- Comprehensive financial, operational & business reporting capability
- IT infrastructure
- Ability to perform data migration from all sources.

As part of its solution, the successful vendor will be expected to provide additional deliverables such as:

- Some form of master data management (MDM) or equivalent, including an optimized, flexible, scalable & efficient data architecture
- Applications, scripts, support & expertise required to affect the timely migration of historical data from legacy internal systems & from stakeholder external systems to the new registry system[5]
- Complete & highly useable system & user documentation
- User, administrator & technical training
- Availability & performance warranties & other features / deliverables described herein.
- Testing & integration

The desired timeline to complete the Registry is on or before December 15, 2023.

The solution must be a cloud-based, commercial off-the-shelf (COTS) application(s) and must reside in a secure Canadian data centre. The solution must be expandable and able to be easily integrated, in future, with a variety of other applications.

The solution must generally conform with the spirit of the Government of Ontario's best practices, including their security and privacy standards, and provide strong IT and IT operational controls, including but not limited to access controls, logging (ex. data auditing), application and data base controls, operating system controls, data validation, error reporting, data quality, program change and maintenance controls, network controls, mobile access controls, telecommunications controls and encryption, if required.

The transitional operating agreement between NCIME and the successful vendor requires NCIME to "protect the information in the registry with technological, administrative and physical safeguards that represent best efforts for the sensitivity of the information, the format in which it is held and the related privacy risks and secure such information against theft, loss and unauthorized use or disclosure".

Lastly, the solution must include the provision of managed services for system operations, evolution and enhancements (including help desk for NCIME staff) for a six-month period, with an option to extend for up to an additional six months (cumulatively).

All of the components of the solution below are required:

2. Enterprise Content Management

Capability	Description
Capture, store label & characterize unstructured & semi-structured data	Able to store, characterize, organize, tag & process unstructured & semi-structured data such as PDFs, documents, legacy files, images, HTML, XML & others including with robust metadata retention
Content search	Able to search across content & content metadata
Security	Generally, conforms with the spirit of Government of Ontario's best practices, including security & privacy standards & is hardened against hacking & other malicious attacks, including mobile devices
Content & archiving	Ability to manage content across its lifecycle & archive / destroy as necessary; privacy & compliance friendly

Integration capabilities	Seamlessly integrates with other registry applications (ex. portals, case management, workflow management) to store, retrieve & manage documents / objects

2.1 Data Management

Cleansed data will be provided to the vendor.

2.2 Financial, Operational & Business Reporting

Capability	Description
Self-serve reporting	Allow business users to manipulate & generate easy to interpret reports for consumption
Mobile accessibility	Access & interact with reports through mobile devices
Visualizations	Readily visualize analyzed data & variances in an easy-to-interpret manner (ex. Dashboards)
Global information system (GIS) integration	Visualize, report & analyze GIS data
Interactive reports	Ability for end-users to interact with reports (ex. drilldowns, filtering)
Data exportability	Ability to export data from reports
Data transformation	Manipulate data through transformations into a format for reporting or visualization
Alerts	Alert appropriate business users if certain metrics drop below or exceed defined limits
Report sharing	Allow for easy sharing of reports both internally & externally through exporting as documents or publication to portal

2.3 IT Infrastructure

The successful vendor must provide detailed information on provisioning the NCIME IT infrastructure and environment to support the new solution.

Capability	Description
Configuration	Description of all major components of the proposed configuration & environment, including hardware, software, network & premises
Availability	Guaranteed availability of the proposed systems
Bandwidth & capacity	Estimated bandwidth & capacity of infrastructure, expressed in terms of ability to meet processing requirements of NCIME
Redundancy	Backup & disaster recovery provisions & capabilities in Canada
Commercial status	Public or private facility; economic viability & track record; escrow & similar arrangements available
Connectivity	Reliability of the connectivity between end users & infrastructure
Security	Generally, conforms with the spirit of Government of Ontario's best practices, including their security & privacy standards & IT hardened against hacking & other malicious attacks, including through mobile. Multi-factor authentication (MFA) for all users is required.
Certification status	CSAE, SSAE, SOC, PCI, ISO 2700, ITIL, FISHMA, HIPPA, other

2.4 NCIME Website

As part of the Registry, NCIME requires the development of a new website that provides easy navigation for users across a variety of devices, platforms, operating systems and browsers to retrieve information and services, to provide links and to provide access to file information from the registry (ex. public reporting). It is the NCIME'S intention that the portal to the Registry would be located on this website.

While further scoping of the website requirements and content will occur with the vendor, the following is needed:

- Final design must provide an easy-to-use, easy to search & simple content management system for the NCIME to manage content independent of vendor support.
- development language must use HTML5 with open APIs for future application integration.
- Website must be fully viewable, useable & accessible from mobile devices.
- Enhanced optimized search engine & website analytics are required to enable NCIME staff to develop reports.
- Best practise programming design standards must be incorporated into the new website.
- A password protected section for NCIME Board & staff.

2.5 Data Migration

Data to be migrated includes any data held by the current NCIME website, other NCIME sources, data yet to be collected and any data held as a result of current NCIME activities. The data to be migrated will be structured and cleansed.

Vendors must develop an approach for data identification, cataloguing, extraction, staging, quality assurance, verification and testing. Provision for end user testing must be made, as well.

2.6 Training & Knowledge Transfer

The successful vendor will be expected to use best efforts throughout the duration of the contract to transfer knowledge to the management and staff of the NCIME. As part of this effort, formal training (user, technical) shall be delivered to the NCIME with respect to the registry capabilities, functionality, skilled and effective use. In addition, training with respect to report generation and analytics must be delivered.

The NCIME supports the use of train the trainer methodology.

2.7 Documentation & Reference Material

The vendor must include in the deliverables complete and up to date documentation (e.g., Wiki) regarding the registry and all associated components, including but not limited to the operating environment, file and data formats, configuration and functionality. It is required that this documentation will be kept up to date throughout the duration of the contract.

All documents produced to support the development, implementation, maintenance and use of the Registry systems shall become the property of the NCIME.

2.8 Managed Services

The vendor must provide managed services for the proposed solution. Services must include, but are not limited to, operational support, bug fixes and evolution of the implemented system through maximizing the use of application functionality and integration with other applications.

Vendor must be available and open to system enhancement work.

2.9 Software Refinement & Maintenance

Vendors will be expected to provide software maintenance. While the preferred solution is COTS (with no customization), should the need for customization arise, the NCIME will work with the vendor to understand the implications and options when developing a custom solution.

2.10 Testing

The vendor must provide a testing and acceptance process for the application. As part of this process, the vendor is responsible for ensuring resolution of all testing in a manner that is satisfactory to the NCIME.

The vendor must develop a plan that includes two distinct phases: one for technical testing and the second for user acceptance testing. The responsibility to ensure the proper functioning and serviceability of the delivered solution shall rest with the vendor.

The vendor must also provide details of its proposed security testing and evaluation program (including penetration testing and threat risk analysis) to be executed as the capabilities of the registry are implemented.

2.11 Security

The successful vendor must assist the NCIME to define and establish appropriate security profiles for registry access, tasks and functions, as well as for the vendor's own technical and support staff. This includes with respect to portal access, mobile access, internal NCIME access and public access.

2.12 Architectures to be Developed

The vendor must provide a plan on how the registry solution will be architected, prior to implementation. This includes all levels of architecture including enterprise, business, application, data, security and technology. In addition, the vendor should indicate the method to be utilized.

3. Requirements

3.1 Security & Privacy

Security plays a critical role in the operation of the registry. Security solutions must meet or exceed NCIME policy guidelines as provided in the RFP (see Appendix C).

3.2 Usability

User experience must include, but is not limited to being, easy to learn, aesthetically pleasing, efficient to use, and open to integration with other applications. Minimal clicks and low loading times are required.

3.3 Scalability & Flexibility

The proposed solution must be scalable and flexible from the system functionality and operating platform perspective. This includes but is not limited to such items as software configuration, operating system performance and data storage capability and capacity.

3.4 Availability

The Registry must meet at least two nines (99%) system availability.

3.5 Ownership of Intellectual Property & Work Product

The NCIME will be the sole and exclusive owner of all intellectual property (IP) and work product emanating from and developed during the course of the contract. The NCIME may, at its sole discretion, enter into a licensing or other agreement with the selected vendor regarding future vendor usage of such IP and work product.

3.6 Warranties – Proposal

When submitting their proposal, NCIME requires that the vendor represents and warrants that all statements, representations and warranties made in their proposal are true and acknowledges that NCIME will rely on the truth of all such statements, representations and warranties in selecting and permitting the vendor to perform the services as described in the vendor's proposal.

3.7 Warranties – Delivered Solution & Services

When submitting their proposal, the NCIME requires that the vendor represents and warrants that all the delivered solution and managed services provided will meet or exceed NCIME's stated requirements and specifications, be fit and serviceable for the proposed usage, meet all applicable industry and government standards and best practices and generally support achieving the NCIME's mandates.

4. The Proposal

Vendors are free to format their information content in any way but should refer to the evaluation criteria of this RFP, the deliverables and the content sections below to ensure that they address all criteria as directly and in as much detail as possible. For ease of evaluation, proposal content should be referenced to the specific RFP subsection, where possible.

4.1 Mandatory Requirements

Vendors must submit their proposals via email in two separate and distinct PDF electronic documents. One electronic document to be marked "technical" must contain details of the proposed solution, services, and approach (ex. no cost information or reference thereto) and the second electronic document to be marked **"**financial**"** must contain only cost information (ex. solution costing details).

4.2. Content of the Technical Proposal

The proposal should contain an executive summary in addition to the other requirements / expectations outlined below. The executive summary should briefly summarize key aspects of the proposal and identify the primary contact person.

The Technical proposal must provide details on the solution, approach and methodology including infrastructure and technologies, services and support, delivery method and generally to answer all areas of the RFP (except financial).

The vendor must describe how they would satisfy the NCIME's requirements in a timely, cost effective, expert phased approach. They must provide their recommended technology solution along with the proposed project management approach, key milestones and a delivery roadmap in a clear and

understandable fashion. They should also be prepared to approach their proposal and the work in a collaborative and transparent manner (and to evidence this approach).

When developing the proposal, it is recommended that the vendors refer to the section above on deliverables and requirements.

The technical proposal must address the following, including but not limited to:

4.2.1 The Solution (ex. the registry including associated environment)

The proposed solution must be clearly identified [ex. listing the software provider(s)] and provide for a solutions roadmap that addresses all components required in the solution (e.g., CRM, ECM, Case Management, EDM, IT infrastructure). The registry includes both the portal for providing information to the NCIME and the public facing website for public reporting.

4.2.2 Project Management Approach & Methodology

The proposal must identify the lead vendor should the proposal be submitted by a joint vendor or consortium.

Vendors must provide information on their formal process to organize and deliver the project deliverables (e.g., project charter, team composition, project management tools) and recommended project approach for each of the deliverables (e.g., Waterfall, Agile).

Vendors must identify whether the product implementation will be done jointly, with a third-party firm or internally (ex. a subcontractor).

- The NCIME recognizes that subcontractors may change throughout the course of the contract; NCIME approval is required for such change.

The proposal must include a proposed project communication plans (ex. between NCIME staff and the vendor, including any subcontractors).

4.2.3 Vendor Qualifications & Resources

Vendors must provide a list of all proposed personnel along with their professional qualifications and related experience. Any detailed resumes or work summaries of key resources must be included as appendices along with professional references for similar engagements. Each vendor must include a description of how they will manage risk associated with the project (e.g., employee turn-over).

4.2.4 Data Migration

Vendors must specify the data migration / ETL automation tools to be used and include a clear roadmap, plan and proposed approach to migrate data to the registry from existing, legacy and stakeholder systems, including timeline estimates.

4.2.5 Training and Knowledge Transfer

Vendors must provide a plan for how they would deliver training and transfer knowledge to NCIME staff (e.g., courses, webinars).

4.2.6 Documentation and Reference Material

As part of the proposal, vendors must discuss and describe the documentation proposed to be provided, and the format thereof (e.g., Wiki). This includes system documentation.

4.2.7 Software Refinement and Maintenance

Vendors must provide a schedule and plan to maintain software within service level parameters.

When submitting their proposal, the NCIME requires that the vendor represents and warrants that all statements, representations and warranties made in their proposal are true and acknowledges that the NCIME will rely on the truth of all such statements, representations and warranties in selecting and permitting the vendor to perform the services as described in the vendor's proposal.

When submitting their proposal, the NCIME requires that the vendor represents and warrants that all the delivered solution and managed services provided will meet or exceed the NCIME's stated requirements and specifications, be fit and serviceable for the proposed usage, meet all applicable industry and government standards and best practices, and generally support achieving the NCIME's statutory mandate.

4.2.8 Managed Services Solution

Vendors must describe their managed services solutions and capabilities. Details of service level management, including but not limited to status reports, operations alerts, problem management process, escalation process, system enhancement requests, testing and production, migration processes and change control processes should be provided.

As part of their proposal, vendors must include a plan to address the following, at a minimum:

- service levels to be delivered throughout the term of the project.
- support service levels to be delivered throughout the term of the project, including incident management and escalation processes.
- software maintenance, configuration, upgrade and enhancement services
- service reporting type and frequency of reporting that will be provided and proposed report delivery method (e.g., vendor self-serve portal)
- Vendors must provide a copy of their proposed service level agreement (SLA) with the proposal; the actual SLA will be finalized during the final negotiation process.

4.2.9 Testing (including sign-off process, technical, quality assurance, end-user)

The proposal must identify any quality assurance the vendor will provide (e.g., testing sign-off process).

4.2.10. Architectures to be Developed.

The proposal must indicate the method to be utilized on how the registry solution will be architected.

4.2.11 Security

The vendor must provide details of its proposed security testing and evaluation program (including penetration testing and threat risk analysis) to be executed as the capabilities of the registry are implemented. Any requirements with respect to any deliverables, process and standards must be addressed in the proposal.

4.2.12 Usability Goals

Vendors must provide details in the proposal on how the solution will meet usability goals (e.g., easy to learn, aesthetically pleasing, efficient to use, along with the key functions that can be used to take full advantage of inherent application capabilities.

4.2.13 Two Nines (99%) System Availability

The proposal submission must provide details on how the solution will meet this requirement and the reporting to provide actual performance information against the final service level agreement (SLA).

4.2.14 Project Roadmap for Implementation (including timelines and key milestones)

Proposals must specifically include a plan to meet the NCIME's immediate priority for an interim registry with capabilities to allow for registration.

The NCIME may negotiate holdbacks or other forms of financial and legal guarantees to ensure delivery of the solution and performance of the services to its entire satisfaction in accordance with the negotiated timelines. For example, liquidated damages may apply in the case of failure to meet agreed delivery dates. As part of their proposal vendors should specify the form and value of assurances that they can provide to the NCIME that the project will be delivered on time and on budget.

4.2.15 Product Road Map

Vendors must include a product roadmap highlighting key application enhancements anticipated and an estimated timeframe. Details of any enhancements of particular interest to the NCIME should be highlighted.

4.2.16 Cost Estimation Model, Delivery Method, Work Breakdown Packages (WBP), Change Request Process and Statements of Work (SOW)

Vendors should submit a sample of their cost estimation model (excluding the vendor's financial information, e.g., the solution costing details) used to calculate project effort, timelines and solution cost estimates as part of their proposal. This is to enable the NCIME to understand the model's basis, derivation and usage. If a recognized formal cost estimation model is used (either paper-based or software) it should be specifically referenced.

Vendors are required to provide details on their proposed delivery method and work breakdown packages (WBP) as part of the proposal. Vendors must also submit details of the proposed change request process, a suggested sample statement of work (SOW) and their proposed WBP signoff and acceptance process.

Sample WBP may include:

- scoping and clarification activity surrounding the level of work required.
- develop basic CRM & portal registration, fee collection & operational reporting capabilities.
- migrate existing data, including historic data.
- enhanced and mature core registry CRM & portal solution capabilities
- enhanced and mature operational reporting capabilities
- implement and integrate case management solution (if applicable)
- implement and integrate content management solution.
- implement and integrate self-service analytics solution.

- data migration activities for the NCIME's historical & each external organization as it winds up.

4.2.17 Refining the Scope and Cost Estimates

The first WBP will be a scoping and clarification activity surrounding the level of work required (ex. complexity) for all WBP provided in the proposal. The initial scoping of WBP will preferably be completed on a time and material basis.

The NCIME envisions that the first step after awarding the contract will be to review all proposed WBP with the successful vendor to confirm high-level cost and time estimates. As the overall project progresses, cost estimates will continue to be jointly reviewed and approved for each individual WBP prior to commencement of work.

4.3 Content of the Financial Proposal

All vendor costs for the proposed solution must be provided in a separate PDF file labelled "Financial". The Financial proposal must include all projected software licensing costs.

4.3.1 Solution Costing Details

Below is a mandatory template to provide the solution costing details.

The one-time implementation costs for the solution must include all vendor costs associated with meeting all deliverables and requirements for the solution as outlined in section 3, including but not limited to:

- staff time
- testing (technical testing & user acceptance testing), including security.
- defining & establishing appropriate security profiles
- configuration
- system set up.
- architecture
- business process design
- training & knowledge transfer
- overall project management (including communications)

As part of the annual licensing costs the vendor must provide complete licensing and cost details on all software proposed to be acquired and all related supporting documentation.

Solution & Costing Details Template		Y1	Y2	Y3	Y4	4Y Total
Portal & CRM	A One-time implementation costs					
	B Annual licensing costs					
Website	A One-time implementation costs					
	B Annual licensing costs					
Data call program	A One-time implementation costs					
	B Annual licensing costs					
Case management	A One-time implementation costs					
	B Annual licensing costs					
Enterprise content management	A One-time implementation costs					
	B Annual licensing costs					
Self-service analytics	A One-time implementation costs					
	B Annual licensing costs					
Enterprise data management	A One-time implementation costs					
	B Annual licensing costs					
Financial, operational & business reporting	A One-time implementation costs					
	B Annual licensing costs					
IT infrastructure	A One-time implementation costs					
	B Annual licensing costs					
Historic data migration	A One-time implementation costs					
	B Annual licensing costs					
Other (specify)	A One-time implementation costs					
	B Annual licensing costs					
Other (specify)	A One-time implementation costs					
	B Annual licensing costs					
Totals						
All one-time implementation total (total of all "As" for all years						
All software licensing total (total of all "Bs" for all years						
Other costs (please provide details for any other costs as applicable)						
IT budget total (total of all A + B for all years, excluding any other costs added by the vendor)						

4.3.2 Rate Cards

Vendors must also include a master rate card for all project activities listed in the deliverables (not including those the vendor has included in the solution costing details) including but not limited to:

- training and knowledge transfer
- creation and maintenance of documentation & reference material
- managed services costs
- software refinement & maintenance
- testing (ex. future software refinements)
- planning, project management, communication and administration

Experience & Knowledge

Vendor should be experienced in similar partnership-based solutions in the past and provide three examples of same.

Budget & Schedule

Issue Date of RFP	June 1, 2023
Deadline for proponent's questions related to RFP	June 20, 2023
Response from NCIME to questions related to RFP	Within 2 business days
Submission Date	June 30, 2023
Rectification Date	July 2, 2023
Contract Award Date	July 14, 2023
Contract Start Date	As soon as contract is signed
Contract Completion Date	March 31, 2024

Budget submissions should be itemized, presented in Canadian dollars, cover all costs, and include applicable taxes.

Rated Criteria

Submissions will be evaluated under the following criteria:

Criteria	**Weighting (Points)**
Relevant Experience and Qualifications	10
Proposed Approach	20
Capacity to meet deliverables required	25
Timeline	10
Pricing*	20
Suitability	15
Total Points	**100**

** Scored using relative pricing formula, see process documentation linked below for full details*

5. Requirements

5.1 Security & Privacy

Security plays a critical role in the operation of the registry. Security solutions must meet or exceed NCIME policy guidelines as provided in the RFP (see Appendix C).

5.2 Usability
User experience must include, but is not limited to being, easy to learn, aesthetically pleasing, efficient to use, and open to integration with other applications. Minimal clicks and low loading times are required.

5.3 Scalability & Flexibility
The proposed solution must be scalable and flexible from the system functionality and operating platform perspective. This includes but is not limited to such items as software configuration, operating system performance and data storage capability and capacity.

5.4 Availability
The NCIME's access to MS365 must meet at least two nines (99%) system availability.

5.5 Ownership of Intellectual Property & Work Product
The NCIME will be the sole and exclusive owner of all intellectual property (IP) and work product emanating from and developed during the course of the contract. The NCIME may, at its sole discretion, enter into a licensing or other agreement with the selected vendor regarding future vendor usage of such IP and work product.

5.6 Warranties – Proposal
When submitting their proposal, NCIME requires that the vendor represents and warrants that all statements, representations and warranties made in their proposal are true and acknowledges that NCIME will rely on the truth of all such statements, representations and warranties in selecting and permitting the vendor to perform the services as described in the vendor's proposal.

5.7 Warranties – Delivered Solution & Services
When submitting their proposal, the NCIME requires that the vendor represents and warrants that all the delivered solution and managed services provided will meet or exceed NCIME's stated requirements and specifications, be fit and serviceable for the proposed usage, meet all applicable industry and government standards and best practices and generally support achieving the NCIME's mandates.

Contract

The successful proponent will be required to enter into negotiations for an agreement with the AFMC NCIME subject to the minimum terms outlined in appendices C. Proponents must indicate in their submission their acceptance of these terms. Proposals submitted without this indication will be disqualified and no further evaluation of the submission will be conducted.

Proposal Submission Instructions

Proposals will be limited to a maximum of 10 pages and submitted in English as a PDF to Danielle N. Soucy, Executive Director, NCIME dsoucy@ncime.ca by date noted above 5:00 p.m. EST, along with a completed RFP Acknowledgement Form. A rectification date will be set as noted above.

Requests for additional information may be directed to the above contact.

Early confirmation of intention to submit is appreciated, those who provide this indication will receive updates should any arise over the request period.

Proposals must be accompanied by completed **Appendix A - Conflict of Interest Declaration.**

Proposals must be accompanied by completed **Appendix B – Confidentiality Undertaking.**

This request for proposals is subject to the process, terms and conditions available here:
https://www.afmc.ca/web/sites/default/files/careers/AFMC_RFP_Process_Terms_and_Conditions.pdf

APPENDIX A: Conflict of Interest Declaration

Vendors biding on the NCIME's RFP for the registry System are required to confirm that they do not have a conflict of interest in relation to the required work.

Declaration
I / we conducted all necessary internal inquiries and investigations to identify and have disclosed in writing to the NCIME any contracts or engagements or payments or purchase orders whether in the name of the vendor, its subcontractors or any otherwise associated entity, with an Industry Funding Organization / Industry Stewardship Organization or with a national service provider to Industry Funding Organizations for the supply of services or goods, regardless of value, from _____ to present.

To the best of or knowledge and belief, except as previously disclosed in writing to the NCIME, there is no

a) financial relationship between any of the directors or officers of the NCIME and the vendor, its subcontractors, or any otherwise associated entity; or

b) relationship of blood or marriage between any of the directors or officers of the NCIME and a partner, director or officer of the vendor, its subcontractors, or any otherwise related entity

I / we understand and agree that failure to fully disclose this information is sufficient cause for the rejection of the vendor's proposal or termination of any contract entered into with the vendor, based on or emanating from such proposal.

DATED this ____ day of _____ 2023

Company: _____

Name: _____

Title: _____

I have authority to bind the Company

APPENDIX B: Confidentiality Undertaking

To: The National Consortium for Indigenous Medical Education

In consideration of the disclosure of the Confidential Information (as hereinafter defined) by the NCIME to the undersigned (the "Recipient"), the Recipient agrees as follows:

1. The term "Recipient" means any vendor, organization or person participating in the NCIME RFP dated _____ and entitled RFP for the Registry System ("RFP"); the Recipient's employees, agents, owners, managers, consultants, associates, subcontractors, and the like are herein collectively referred to as the "Representatives".

2. The term "Confidential Information" means any information disclosed by the NCIME to the Recipient at any Information Session or otherwise, in respect of the RFP.

3. The information may be in the form of draft reports, final reports, Data call or other survey forms, data entered into a database, analysis and interpretation of data, supporting documentation, personnel information, financial information, internal memos, and documents, electronic and hard copy correspondence and all other information and verbal and/or written communications.

4. Confidential Information does not include any information which:

(a) was at the time of disclosure or thereafter became part of the public domain or was readily available to the public otherwise than by reason of a breach of this Agreement

(b) at the time of disclosure by the NCIME to the Recipient or thereafter, was known to or within the possession of the Recipient or was independently developed by the Recipient without the Confidential Information disclosed by the NCIME, or

(c) was required to be disclosed by law.

5. The Recipient shall not disclose and shall ensure that its Representatives do not disclose the Confidential Information without the prior written consent of an authorized representative of the NCIME and shall use and cause its Representatives to use the Confidential Information only for the purposes set out below.

6. The Recipient and its Representatives may use the Confidential Information to undertake the following tasks:

(a) develop a proposal for the NCIME's consideration with respect to the RFP

(b) develop and submit deliverables (e.g., reports) to the NCIME for the project described in the RFP

(c) consult with members of the NCIME, as necessary, to inform them about their deliverables

7. The Recipient agrees that it shall use all its best efforts and exercise appropriate due diligence, to safeguard the Confidential Information from misuse, loss, theft, publication, destruction, or the like, and has implemented suitable internal controls to do this.

8. This Agreement shall be governed by and interpreted in accordance with the laws of the Province of Ontario.

DATED this ____ day of _____ 2023

Company: _____

Name: _____

Title: _____

I have authority to bind the Company

APPENDIX C: IT Guidelines for Registry Development

These Guidelines have primarily been developed for the purpose of informing the development of a Registry for the Authority. The primary objective supported by this Guideline is to protect and ensure the integrity of information that is in the possession of the Authority.

Information Classification

The Authority will utilize the following Government of Ontario Information Security & Privacy Classification System to classify the type of data the Authority has and will have in its possession.

Currently the Authority has in its possession "Low Sensitivity" or "Unclassified" information.

Based on the Authority's mandate, it is expected that the Authority will have in its possession, at the most, "Medium Sensitivity" information once the Registry is live (ex - registered user, user demographics data, contracts).

This Guideline has been developed based on the Authority in future having in its possession "Medium Sensitivity" information.

Registry Guiding Principles

In the development of the Registry, the Authority will:

- Align the solution with the spirit of the Ontario Open Government Initiative.
- Build scalable & flexible data management & application capabilities to meet implementation timelines & future regulatory requirements
- Ensure that applications implemented address data security & privacy requirements
- Ensure that applications & infrastructure are implemented in the most cost effective & efficient manner
- Utilize cloud-based solutions for applications & infrastructure
- Use commercial off-the-shelf (COTS) applications with no/minimal customization

Explore innovative vendor contract arrangements to ensure business requirements are delivered in a shared-risk environment.

- Identify, validate & implement potential value-added services

Management of Stored Information

Data Management

Data stored electronically will be subject to information lifecycle requirements and will be purged or archived after it reaches end-of-life for each of the following:

1. Business information residing in applications
2. Business information residing in documents on file servers
3. Physical documents

The retention period for each type is the minimum required by legislation or regulation in order to minimize potential information exposure. Information of a transactional nature or that is no longer needed is purged periodically.

Application Hosting

Business applications (e.g., the actual Registry, unstructured data, case management information, and internal financial information) are hosted and operated by third-party data centres (i.e., cloud solution providers).

The data centre is located in Canada.

Security Requirements for Data Centre

The following are the minimum requirements for a data centre to be utilized by the Authority:

- Physically secure data centre:
    - Physical control on access by data centre employees as well as customer visitors, logging of entry and exit from data centre, video surveillance
- Data centre employees have no direct access to system
- Employs industry-standard practices around:
    - Password management, expiry, and complexity
    - Change control process to manage change to customer environment
- Intrusion Detection Services
- Anti-Virus Services
- Server operation, including monitoring and patching
- Data Centre manages security incident response to security events.
- Data Centre performs an annual security audit and provides detailed audit results to the NCIME

Back-up & Recovery of Information Requirements for Data Centre

Multiple levels of backup and failover protect the integrity of the Registry. Information is regularly backed up and backups sent off-site so that data loss from hardware failure or operations failures can be recovered. The data centres each have data centre failover in case of complete loss of a data centre.

Computer servers are backed up regularly. Backups are sent to failover data centres so that backup data is physically separated from the servers being backed up. Backup data is sent by secure private networks; there is no physical backup media that could be misplaced or intercepted.

All servers are backed up daily; backup times are staggered and outside of business hours. Email servers are backed up hourly.

In the event of a failure of an entire data centre, operations will be transferred to a failover data centre. Services will resume from the failover data centre and may operate there for as long as needed.