Request for Proposals (RFP) For

All-In-Consent – Core Engine Build

ISSUED BY THE

NEW YORK eHEALTH COLLABORATIVE

APPLICATION INFORMATION	
CONTACT	NYeC
EMAIL ADDRESS	AICCoreEngineRFP@nyehealth.org
SUBMISSION DEADLINE	September 6, 2022 5:00 PM EST

All correspondence and proposals should be submitted via email directly to the mailbox listed above and include **All-In-Consent Core Engine** in the subject line.

I. STATEMENT OF PURPOSE

New York eHealth Collaborative (NYeC) is seeking applications from Managed Service Providers (MSP) to architect, execute, and support a patient consent solution for a new consent model in New York State, known as All-in-Consent (the Solution). The Solution consists of two parts, the Centralized Consent Hub (CCH) and the implementation of a Master Patient Index (MPI). Respondents can submit proposals utilizing sub-contractors to achieve outcomes for this RFP. The use of subcontractor(s) cannot exceed 50% of the effort for this project[1].

a) The CCH, which will be developed as a Microsoft Azure application, utilizing Azure components, and an on-prem gateway, queuing infrastructure, and endpoints. The application must have the capacity to expose API endpoints for stakeholders to consume and must also have the capacity to consume stakeholders' API endpoints to exchange consent data.

b) Implementation of a Master Patient Index (MPI) for the consent feeds. MPI shall receive Consent feeds (CCH Master Patient Index (MPI)), Application Programming Interfaces (APIs), and Queue which will be developed using MDM-based MPI for the patient identity management, and APIs will be developed and configured on DataPower (On-Prem) and Queue capability via IBM MQ (On-Prem). Respondent shall describe their MPI plan, including which MPI software vendor they plan to use, and the one-time and ongoing costs to operate this MPI.

The Solution must support scalability and high availability for future use cases, operational, and disaster scenarios.

[1] If the applicant plans to retain one or more subcontractors to perform work under an award pursuant to this RFP, the applicant understands and acknowledges that the applicant shall be responsible for any failure on the part of any of its subcontractors to comply with the terms and conditions of any agreement between the applicant and NYeC that are applicable to the applicant as if such terms and conditions were applicable to such subcontractors. All subcontractors retained by the applicant to provide services under any agreement with NYeC will provide services at the direction of the applicant, and the applicant shall: 1) maintain full responsibility for subcontractors meeting all of the applicant's obligations under any agreement with NYeC, and 2) indemnify and hold harmless NYeC and its representatives and NYSDOH from any and all claims arising from or relating to the services provided by subcontractors, including, without limitation, claims for payment in connection with the provision of Services and Deliverables.

II. INTRODUCTION

NYeC is working to improve healthcare for all New Yorkers through innovative health information technology and exchange (*HIT and HIE*). Founded in 2006 by healthcare leaders, NYeC is a 501(c)(3) non-profit organization and the State Designated Entity (SDE) in New York charged with the leadership, coordination, and administration of the Statewide Health Information for New York (SHIN-NY), the state's public health information exchange (HIE). In that capacity, NYeC works as a public/private partnership with the New York State Department of Health (NYS DOH) on the development of policies and procedures that govern how electronic health information in New York State is shared via the SHIN-NY, an innovative "network of networks" that interconnects New York's regional health information organizations (Qualified Entities or QEs). QEs allow participating healthcare professionals, with patient consent, to quickly access electronic health information and securely exchange data with any other participant in the state.

Additional information regarding NYeC can be found on the NYeC website www.nyehealth.org.

III. BACKGROUND INFORMATION

New York (NY) is an opt-in state for patient consent, and currently, consent is captured in a wide variety of methods, and the scope of that consent varies widely. Consent may be given and respected within a single organization, or consent may be respected within a region. NY seeks to enable a model whereby patients could grant consent, and have their consent declaration respected broadly by HIEs, Payers, Providers, and other healthcare professionals.

NYeC is responsible for developing the central consent service responsible for receiving/sending and responding to Application Programming Interface (API) requests for consent status. This new consent approach is an All-In-Consent (AIC) model. In that context, NYeC will require an enterprise-wide (SHIN-NY) application to collect and share consent across health entities. The AIC model will allow patients in New York State to grant consent for SHIN-NY data access to all their current and future treating providers and insurance plans through a single statewide form or electronic consent process. The SHIN-NY will partner with external organizations (such as health plans) to provide opportunities for patients to grant AIC. To manage this consent model effectively, QEs will share AIC data across the state to maintain an accurate and consistent AIC status for a given patient.

As currently proposed in the AIC model, external organizations such as state agencies, health insurance companies, and large health systems will offer opportunities to the consumers they serve to grant AIC during administrative processes such as enrollment or registration. When individuals decide to grant AIC, the organizations will notify their local QE or NYeC. QEs will process and store the AIC status change event locally and will also send the status change information to a CCH maintained by NYeC. The CCH will store and process the AIC status change and will send a notification to any QEs that have those patients in their MPI. Patients will also be able to change their AIC status through the use of a separate consent form that will be housed in a centralized SHIN-NY website, or possibly through AIC collecting organizations. In addition, when the statewide Master Patient Index (sMPI) links, merges, splits, or moves patient identity records, the CCH will notify QEs if those actions affect the AIC status of patients in the QEs' MPIs. QEs will also be able to query the CCH when needed to determine the current and historical AIC status of specific individuals. These combined processes and capabilities will ensure that a patient's most current AIC status is known or available to all QEs.

NYeC, as the State Designated Entity (SDE) of the SHIN-NY, is charged with the implementation of AIC. As part of this initiative, NYeC is seeking an MSP to partner with on the development of a technical solution and support for AIC implementation. This initiative will be implemented in multiple phases as described in more detail in the project scope and content sections of this RFP.

Phases of building the Centralized Consent Hub

1. NYeC will develop core infrastructure, queuing, and APIs.
1. Partner selected in this RFP will develop and integrate Consent Core Engine (MS Azure will be the PASS environment for the solution).
2. Partner selected in this RFP will develop and integrate MPI implementation using MDM and its integration with CCH and sMPI.
3. Partner selected in this RFP will develop and integrate an internal web-based management application to search, filter, view, and review the consent from the CCH repository. This admin tool will also need to allow NYeC staff (or AIC service center staff) to edit/change a patient's AIC status. The audience for this is an administrative professional tasked with processing forms sent in through postal mail.

The API Gateway and Queuing Capability aspects of the CCH will be designed and developed on-premises (in the NYeC data center) by the NYeC internal team. Below is a summary of the high-level requirements for both components.

a. Consent Core Engine (MS Azure will be the PASS environment for the solution which needs to be integrated with APIs and queuing infrastructure.) The diagram below shows the high-level flow of the consent data. The middle part of the diagram depicts the consent core engine which is integrated with Queue and sMPI.
b. An internal web-based management application to search, filter, view, and review the consent from the CCH repository. This admin tool will also need to allow NYeC staff (or AIC service center staff) to edit/change a patient's AIC status. The audience for this is an administrative professional tasked with processing forms sent in through postal mail.
c. MDM-based MPI build and configuration for managing the patient identification (MRN) and integrating it with the existing sMPI and CCH.
d. Coordinating with the internal team for creating and configuring the APIs for CCH using the DataPower secure gateway.
e. Coordinating with the internal team for creating the queuing capability for CCH data ingestion using the IBM MQ.
f. A management console by which the administrative functions of the platform can be performed. The audience is a typical IT System Administrator.
g. Sufficient logging as is required by NYeC regulation and HIPAA related to patients' change in consent status.
h. Sufficient technical telemetry data to provide information about system performance to enable an IT administrator to find and resolve typical issues.

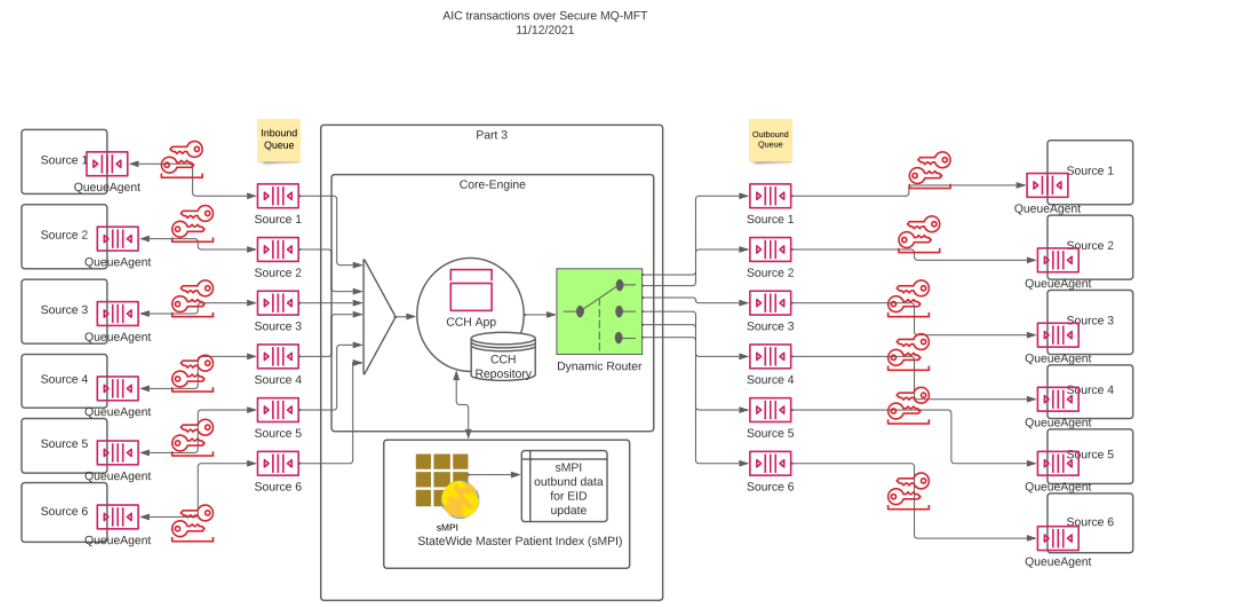

Diagram – High-level consent data flow

IV. ELIGIBILITY CRITERIA

Applicants (referred to as vendors) and/or subcontractors must meet the following required qualifications:

- Able to register in the Federal System for Award Management (SAM) prior to commencement of work, if selected, and;
- Able to complete the New York State Vendor Responsibility Questionnaire, and;
- The selected vendor and/or subcontractor(s) will be required to adhere to certain New York State grant contracts and confidentiality requirements specific to the initiative. These requirements will be outlined in the vendor contract, and;
- The selected vendor and/or subcontractor will also be required to agree to NYeC's Security Requirements Addendum (Appendix B), which includes but is not limited to, the requirement that no NYeC Proprietary Data, including PHI and PII, may be transmitted, accessed, or stored outside of the United States, including storage via server storage, backup, printing, photography, copy, paste or similar functions, and;
- The vendor must submit demonstrable evidence on behalf of the vendor and/or subcontractor of creating a combined total of at least 5 Azure Platforms as service APIs that operate at a scale of more than 25,000 transactions per day with a response time of <500ms, and;

- The vendor must submit demonstrable evidence on behalf of the vendor and/or subcontractor of using Continuous Integration/Continuous Deployment pipelines, using automation such as but not limited to Azure DevOps, and;
- The vendor must submit demonstrable evidence on behalf of the vendor and/or subcontractor of using one or more tools to create and execute automated test scripts on at least five (5) enterprise-class applications, and;
- The vendor must submit the demonstrable evidence on behalf of the vendor and/or subcontractor of operating a 7x24 support structure for enterprise-class applications, including executing against a set of defined Service Level Agreements (SLA), and;
- Consent Core Engine and all related components must be built in NYeC-owned cloud and infrastructure and must be handed over to the NYeC team along with all configurations, build, and operational documents; and
- The vendor must submit demonstrable evidence on behalf of the vendor and/or subcontractor of setting up at least 5 MDM-based systems building the Master Patient Index (MPI) that operates at a scale of more than 2,500,000 transactions per day with a response time of <500ms, and;
- The vendor must submit demonstrable evidence on behalf of the vendor and/or subcontractor for setting up the IHE web services and integrating them with IHE profiles such as PIX Add, Update, Merge and Query, and Demographics query (XCPD), and;
- The vendor must submit the demonstrable evidence on behalf of the vendor and/or subcontractor for setting up the Message broker and reader for ingesting the patient demographics to MDM using ADTs for Add, Update, Merge, and delete. Evidence should also include validation scripts.

Preferred qualifications:

If available, NYeC encourages applicants to submit evidence, for the vendor and any subcontractors, of external security audits or certifications such as:

- HITRUST Certification
- ISO 27001

V. MANDATORY REQUIREMENTS

All applicants and subcontractors must submit a completed Cloud Security Alliance Consensus Assessment Initiative Questionnaire v4 (CAIQ v4) (available at: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/) and NYeC's Third-Party Security Risk Assessment Questionnaire. Please email aiccoreenginerfp@nyehealth.org for a copy of NYeC's Third-Party Security Risk

Assessment Questionnaire. If any subcontractor(s) fails to meet these mandatory requirements, NYeC will automatically have to reject the applicant's proposal.

VI. SCOPE OF WORK

NYeC is planning to implement the All-In Consent Model in multiple phases. The vendor will be expected to estimate the efforts per phase and to create a consolidated estimate of overall project cost and level of effort, broken out by vendor/subcontractor responsibilities. The following outlines the phases of the two components.

1. **Initial Phase: Architectural and Implementation Design**

   Requirement walkthrough and designing of the complete architecture and solution covering phases one and two as described below. This phase will also include crafting the service level agreements for all the services and APIs identified as part of the design and architecture. As part of the response, describe the typical artifacts produced during design. If possible, provide examples that have been redacted as appropriate.

2. **Phase One (Milestone one): Patient Enrollment Consent Management - Collect and submitted via trusted sources (QEs)**

   As described in the background section, patient consent will be collected by external organizations for SHIN-NY Participants and electronically submitted to their associated QE(s). The receiving QE will store the information as per its current consent management process and submit the same information to CCH. The CCH will store and distribute the consent across the SHIN-NY based on sMPI results about the patient.
   As part of the proposal, vendors will include resource(s) to build an API to exchange the consent information with stakeholders, i.e., NYeC should expose the API to accept the feed from stakeholders and NYeC should be able to consume stakeholders' API to push the consent notifications.

   Query

   As part of the proposal, vendors will plan to develop and integrate the ability to query the CCH for any patient's current consent detail and history of the patient's consent. The expectation as part of the Query implementation is that any stakeholder should be able to query the CCH repository using the Query/Search API based on defined parameters for:

   1. Current status of the consent for a patient
   2. History of the consent for a patient.

Web-based application to view and review the consent data

The development of a secure web-based application to search, filter, view, review, and edit the consent based on the user role from the CCH repository. This is internal to the NYeC team and used for troubleshooting and operational purposes.

As part of the proposal, the vendor will update the architecture design diagram contained within this RFP with lessons learned and recommendations for future implementation.

3. **Phase One (Milestone Two): Patient Enrollment Consent Management – collected and submitted directly to CCH (NYeC) – built on NYeC data center**

   Centralized consent management will be extended to external entities such as health plans to directly connect and submit the consent data to the CCH to process the patient's consent and distribute it to all associated QEs. The expectations for this phase are to:

   1. Setup a MPI using MDM-based technology to consume the patient demographics to create the Patient (collection of MRN's). This would be referred to as CCH MPI.
   2. Possible methods to feed CCH are CSV Files or via CCH API. Demographics data from the feed should be fed to CCH MPI.
   3. Open the CCH MPI APIs to be consumed by the CCH API for the participant to feed the data using CCH API.
   4. Setup Message broker and reader to feed the data via the file ADT (CSV data transformed to ADT).
   5. Build the process and tool to extract and feed the CCH MPIs to sMPI, where CCH MPI will go through the matching process to link with sMPI sources.
   6. After MRN (MPI) is created in CCH MPI, submit the consent data to CCH for storing and distributing the consent to all QEs wherever that patient exists.

4. **Phase Two (Milestone one): MPI Triggered Consent Management**

   This phase requires extending the phase one solution and incorporating the MPI-triggered workflow to synchronize the consent across the SHIN-NY enterprise that includes all QEs based on an architectural design done in the initial phase and lessons learned in phase one. The expectations for this phase are to build:

   1. A service to read, process, and store the sMPI changes to storage (database) for patients' status.
   2. Evaluate the consent of each patient whose status has changed in MPI
   3. Distribute the consent to all concerned stakeholders

5. **Enhancement and Support**

NYeC expects application enhancement and ongoing support for the six (6) months following deployment of the solution in production to be included in the initial RFP response. The requirement is six (6) months and should include five (5) mid-size enhancements and application support. This should be included in the RFP as deliverable Production support and should include any issues troubleshooting, resolution, and maintaining the SLA crafted as part of the design phase (e.g., performance (>500ms/transaction), uptime (99.999)) expectations.

VII. CURRENT ARCHITECTURE, APPLICATIONS, AND PROCESSES:

- **Centralized Consent Management**: This is a new system to be designed and developed as part of this RFP process. It is targeted to be developed on the Microsoft Azure platform and integrated with API Gateway and Queue on Prem.
- **Statewide Master Patient Index (sMPI)**: NYeC hosts and operates the sMPI which is the patient registry. The CCH shall integrate with the sMPI in order to find patients across the SHIN-NY network.
- **API Gateway:** NYeC hosts API Gateway which will be used for opening the endpoints for QEs.
- **Queue pipeline**: NYeC is currently building the queuing infrastructure, which will be extended for the AIC application, and plugged between Gateway and the CCH.

VIII. OBJECTIVES OF THE PROJECT:

NYeC has established the following primary objectives for the project –

- Understand the requirements and architect and design the solution;
- Integrate the new solutions with the existing Gateway and Queuing infrastructure for securely exposing the endpoints for stakeholders to consume;
- Consume the stakeholder's endpoint for pushing the consent notification for any update;
- Security compliance;
- Excellent ongoing support and customer-centric approach;
- Ability to scale and perform based on the growing volume of transactions;
- High availability should be part of the solution and;
- Ability to enhance and add new features as per business needs.

IX. CONTENTS OF PROPOSAL

The following section outlines the contents that should be included in a proposal in response to this RFP.

1. Applicant Overview and Qualifications:
   The proposal should provide a general overview of the applicant's and any subcontractor's capabilities, resources, and experience. Applicants should include a brief narrative that demonstrates:
   - The organization's clear understanding of the scope of the project.
   - The vendor's/subcontractor's capabilities and strengths as it relates to this project.
   - A description of the vendor's/subcontractor's operation; facilities, business, and objectives, and the number of employees dedicated to and/or who have experience with Azure-based application development and integration with on-prem gateway and queue.
   - A high-level description of the projects and technical resources that have worked on enterprise-wide applications demonstrating the ability to handle enterprise-wide applications.
   - Demonstrable evidence for the eligibility criteria outlined in section IV. A description of the vendor's operation; facilities, business, and objectives, and the number of employees dedicated to and/or who have experience with MDM-based MPI, and integration with DataPower, and MQ based application development and MS Azure-based application.
   - A high-level architectural design and implementation-related artifacts that demonstrate the ability to perform enterprise-wide design and implementation.

MS Azure (For Consent Core Engine Build)

- A description of at least five other Azure projects for which the vendor and/or subcontractor used Azure cloud for developing and integrating such services (rest APIs) using Node JS for business logic and MS SQL and Mongo DB as backend storage.
- A description of how the vendor and/or subcontractor approaches continuous build and deploy and staging and final production deployment using Azure Dev Ops native tools to establish and then change the DEV/TEST and PROD landscapes.

- Estimated timeline to set up DEV/TEST and PROD development landscape once the contract is executed. The project must be completed by 6/01/2023.[2]
- A description of how the vendor and/or subcontractor integrates Azure application monitoring and audit information with on-prem databases.
- A description of how the vendor and/or subcontractor worked with the customer(s) to establish security structures – ideally in a way that limits access based on the individual, the data set, and the least privileges concept (role-based access) for the development pipeline.
- A description of how the vendor and/or subcontractor worked with the customer(s) to establish on-premises datacenter connectivity for integrating the application with API Gateway and backend (such as services, databases, etc.).
- A description of how the vendor and/or subcontractor has implemented the audit for collecting and storing the defined set of data and provided a report on-demand request.

MPI Expertise (For MPI Implementation)

The preferred applicant provides the following information:

- Statewide MPI is built on IBM Master Data Management (MDM) product. A description of projects (use cases or scenarios) where the vendor and/or subcontractor has demonstrated the MDM skill set to achieve the defined goal (mentioned above in phase 2 and future phases).
- Statewide MPI services request and response are XML based, a description of projects or work done consuming XML-based services and converting XML responses to JSON and using it in the application which could be Node JS-or any other platform.

General

Additionally, the applicant must provide the following information:

- Identify the name, title, and contact information of the point of contact for this proposal.
- Provide resumes for all the lead resources including subcontractors.
- Provide three (3) references of similar projects undertaken in the previous 5 years.

[2] Project Completion shall include, but not be limited to, successfully importing consent from at least two pilot health plans, and distribution of those consent status conveyed to QEs and at least two technology platforms connected to the APIs. This is in anticipation of receiving 5M plus consent records in Q4 from the state.

Reference Template	
Contact Name:	
Company:	
Title:	
Phone:	
Email:	
Brief description of the project:	

2. Approach and Plan**:**
   The proposal should include a thorough, detailed approach and plan to architect, execute, integrate, and QA a solution for collecting, storing, and distributing consent across the SHIN-NY with sufficient support.
   - The plan and approach should specifically address:
     - Architectural Design and implementation artifacts depicting components communication and workflow
     - A feasible solution to set up the CI/CD for project development and deployment.
     - A feasible solution to build a Centralized Consent Engine and integrate it with on-premises API Gateway and Queue infrastructure developed by NYeC internal team.
     - An approach to specifically address knowledge transfer to NYeC technical staff for NYeC to support ongoing maintenance and support upon contract completion.
     - Integration of the application with on-prem database, backend applications, API Gateway, and queuing capability (IBM MQ).
     - Weekly status reports/touchpoints.
     - Plan for ongoing maintenance, support, and customer-centric approach to providing this service for 6 months after project completion. This should include a description of support services to be available 24/7 when issues arise as well as collaborating with the NYeC IT team to enhance services, as necessary.
     - Plan an approach to address information security in all aspects of the project, and as may be required by NYeC, including but not limited to architecture, execution, integration, and implementation.
     - Implementation of MDM-based Master Patient build and configuration
     - MDM installation and configuration including the algorithm builds and tuning.

    - MDM MPI APIs deployment and configuration (Web Services and IHE Web Services)
    - Inbound and Outbound Message Broker and Reader configuration
- The plan must include a project management outline for achieving the requirements of this RFP, including planned project management tools, approach, and collaboration and partnership with NYeC's Enterprise Project Management Office, where appropriate.
- Vendor and/or subcontractor project management team would collaborate with NYeC Enterprise Project Management Office project administration purposes.
- The plan must include a high-level project plan and project execution summary plan
- The plan must contain the following details:
    - Architectural Design and technical implementation guide build phase
    - List of implementation artifacts
    - Approach and format of Quality assurance phase
    - Approach and plan of Deployment and UAT Phase
    - Maintenance and Support structure

3. Cost**:**

The proposal must include a detailed budget for total project implementation cost (with clear indication of any subcontractor costs), a breakdown of software and services to be provided, and hourly rates for maintenance and types of support to be provided for the first six months after project implementation completion. Payment milestones will be negotiated based on the implementation timeline agreed to by NYeC and the successful applicant with completion by 6/1/23.
The following components should be considered while estimating the cost

- Initial assessment and architectural design
- Implementation of the solution
- Deployment strategy and tools
- 6 Month maintenance and Support

4. Security**:**
All vendors and subcontractors must submit a completed Cloud Security Alliance Consensus Assessment Initiative Questionnaire v4 (CAIQ v4) (available at: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/) and NYeC's Third-Party Security Risk Assessment Questionnaire. Please email

aiccoreenginerfp@nyehealth.org for a copy of NYeC's Third-Party Security Risk Assessment Questionnaire.

X. APPLICATION PROCESS AND TIMELINE

Proposals will be evaluated by a selection committee as determined by NYeC. Proposals that do not address all the criteria outlined below may not be evaluated by NYeC.

Proposal submissions are due on or before September 6, 2022, by the close of business (5 p.m. EST). Organizations may only contact NYeC using the email address AICCoreEngineRFP@nyehealth.org for all matters concerning this RFP.

NYeC will host a bidder's conference to provide interested and eligible vendors the opportunity to ask questions regarding the RFP. This will take place virtually on July 19, 2022 1:00 – 2:00 PM EST. Interested vendors must register for the bidder's conference. Submit the request to attend to AICCoreEngineRFP@nyehealth.org to receive a link to the virtual conference.

If you have questions about the application, please submit those questions to the designated mailbox noted on the cover page of the RFP by July 21, 2022**.** NYeC will post all questions received and answers to those questions on our website, along with notes from the Bidders Conference at, https://www.nyehealth.org/rfis-rfps/, by August 1, 2022**.**

Applicants may only contact NYeC through the designated mailbox, and may not contact any NYeC staff, NYeC board members, New York State Department of Health staff, or any other stakeholders regarding this proposal in the period between the issuance of this RFP and the notice of award. Any oral communication will be considered unofficial and non-binding regarding this RFP and subsequent award. Additionally, attempts to contact others, as listed above, may result in disqualification from the process.

NYeC reserves the right to amend or cancel this RFP at any time prior to a signed contract. NYeC is not responsible for any costs incurred in the preparation of a response to this RFP.

Please submit your application(s) in Microsoft Word format using font size 12 with a maximum of 15 pages. References, certification letters, and any relevant supporting

documentation will not count toward the 15-page maximum. All valid applications must include all sections identified in the evaluation criteria.

TIMELINE

ACTIVITY	DUE DATE
Release of RFP	July 12, 2022
Pre-Bid Conference	July 19, 2022 @ 1:00 PM EST
Submission of written Questions	No later than July 21, 2022
Distribution of pre-bid conference minutes and Responses to Written Questions	August 1, 2022
RFP Proposal Submissions	September 6, 2022, 5:00 PM EST

XI. METHOD OF AWARD

Success in this process will result in a contract that will cover the period starting in September 2022, where the project should be completed by 6/01/2023[3] and the maintenance support should be provided through 6 calendar months post go-live. All proposals will receive a score based on the evaluation criteria outlined in the RFP. NYeC reserves the option to select finalists for one-on-one interviews. The use of subcontractor(s) cannot exceed 50% of the effort for this project. If the applicant plans to retain one or more subcontractors to perform work under an award pursuant to this RFP, the applicant understands and acknowledges that the applicant shall be responsible for any failure on the part of any of its subcontractors to comply with the terms and conditions of any agreement between the applicant and NYeC that are applicable to the applicant as if such terms and conditions were applicable to such subcontractors. All subcontractors retained by the applicant to provide services under any agreement with NYeC will provide services at the direction of the applicant, and the applicant shall: 1) maintain full responsibility for subcontractors meeting all of the applicant's obligations under any agreement with NYeC, and 2) indemnify and hold harmless NYeC and its representatives and NYSDOH from any and all claims arising from or relating to the services provided by subcontractors, including, without limitation, claims for payment in connection with the provision of Services and Deliverables.

[3] Project Completion shall include, but not be limited to, successfully importing consent from at least two pilot health plans, and distribution of those consent status conveyed to QEs and at least two technology platforms connected to the APIs. This is in anticipation of receiving 5M plus consent records in Q4 from the state.

XII. EVALUATION CRITERIA

1. **Applicant Overview (Executive Summary) & Qualifications (Experience): 30 POINTS**
   Please see Section X. Contents of Proposal for required information.

2. **Approach and Plan: 55 POINTS TOTAL**
   Please see Section X. Contents of Proposal for required information.
   - **Azure-based development and deployment 10 POINTS**
     Ability to set up the CI/CD for this project and develop, deploy, and integrate with on-prem Gateway and Queue.
   - **AIC-Implementation and Support and Enhancement Plan 15 POINTS**
     Implementation of the AIC Core engine: Architectural design and Implementation approach and plan
   - **AIC – Integration with internal backend systems/applications, databases Plan 10 POINTS**
     Integration plan for consuming internal (on-prem) systems/applications and databases for completing workflows (for example Integration with sMPI and connection with databases for storing and querying the consent).
   - **MDM-based MPI – Build and configuration 20 POINTS**
     Implementation of MDM-based Master Patient build and configuration:
     - MDM installation and configuration including the algorithm builds and tuning.
     - MDM MPI APIs deployment and configuration (Web Services and IHE Web Services)
     - Inbound and Outbound Message Broker and Reader configuration

3. **Cost: 15 POINTS**
   Please see Section X Contents of Proposal for required information.

4. **Security: 0 POINTS**
   Applicants will only be considered for review if they comply with NYeC's security requirement to submit a current (within the past 12 months) SOC 2 Type 2 audit report for the vendor and/or subcontractor. Additionally, all vendors and subcontractors must submit a completed Cloud Security Alliance Consensus Assessment Initiative

Questionnaire v4 (CAIQ v4) (available at: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/) and NYeC's Third-Party Security Risk Assessment Questionnaire.

APPENDIX A - Glossary of Terms

All-In Consent (AIC) – A SHIN-NY consent model that allows people to grant access to their SHIN-NY health records to all current and future treating providers and health plans through a single form.

Source – A QE or health entity that receives the initial AIC enrollment information (or AIC status change notification) from an AIC Collecting Organization.

Centralized Consent Hub (CCH)– The SHIN-NY technical solution for receiving AIC status change notifications from Source QEs, logging and storing the information, processing consent status updates, and distributing AIC information as outlined in this document.

Consent Core Engine (CCE)– The consent Core Engine is the application handling the core consent management functionality and should be built on the MS Azure cloud infrastructure owned by NYeC.

Destination – Any QE or health entity that receives an AIC status update from the Centralized Consent Hub.

Statewide Master Patient Index (sMPI): An Enterprise system Master Data Management (Patient demographics registry) that collects and maintains the patient's demographics and exposes endpoints to post and get the required patient information. It is a typical Master Patient Index used in any healthcare system.

API Gateway: This is a typical Gateway used for security and external system-to-system communication

APPENDIX B - Information Security Requirements Addendum

Information Security Requirements Addendum

NYeC ("**NYeC**") and _____ have entered into an Agreement for services as of _____, 20__ (the "**Agreement**") which is incorporated herein by reference, and hereby agree to the following additional terms and conditions which shall be effective as of the _____ day of _____, 20__.

1. Definitions

The following terms have the indicated definitions and meanings:
"**Addendum**" or "**Requirements**" means this Information Security Requirements Addendum.
"**Breach**" shall include but is not limited to: (i) any use, loss, destruction, compromise, access, disclosure, collection, retention, storage, transfer and/or other act or omission with regard to Proprietary Data that is unauthorized, invalid or inconsistent with the Agreement, this Addendum and/or any applicable law, regulation or standard and/or otherwise inappropriate; or (ii) any act or omission, that causes non-compliance with these Requirements; or (iii) any "breach of the security of the system" as defined in NYS General Business Law §899-aa.
"**Consultant**" as used in this Addendum means the Consultant identified in the header above.
"**Approved Consultant Resources**" shall include, but not be limited to, any contractors, subcontractors, consultants, temporary associates or other third parties which Consultant utilizes, with NYeC's prior written approval, to Process (as defined herein) Proprietary Data and/or provide Services (as defined herein) to NYeC under the Agreement.
"**Consultant Employees**" shall include any employees of consultant who are utilized by consultant to Process Proprietary Data and/or provide Services to NYeC under the Agreement.
"**Process**" or "**Processing**" means any action taken by Consultant, Consultant Employees and/or Approved Consultant Resources in relation to Proprietary Data, to include access, collection, use, retention, storage, transfer, disclosure, destruction, and any other operation.
"**Proprietary Data**" means data or information provided by or on behalf of NYeC, regardless of form or media and regardless of whether it is so designated by NYeC, which includes, but is not limited to:

a) personally identifiable information ("PII"), including, but not limited to, an individual's: (i) Social Security number; (ii) date of birth; (iii) home address; (iv) home/personal telephone number; (v) home/personal email address; (vi) user passwords or personal identification numbers ("PIN"); (vii) driver's license or other state or federal identification number; (viii) financial account information; (ix) health or medical information, including but not limited to individually identifiable health information and protected health information ("PHI") as such terms are defined in 45 CFR §160.103; (x) insurance ID number; or (xi) biometric data;
b) private information as defined in NYS General Business Law §899-aa.

c) NYeC employee data, including, but not limited to: (i) human resources data (e.g., Social Security number, date of birth, performance reviews, medical information, health information, family information, etc.); or (ii) compensation data;
d) NYeC corporate financial data, including, but not limited to, information on NYeC sales, sales projections, and corporate strategies, which have not been released to the public;
e) NYeC application or system user ID and passwords;
f) data which is specifically identified by NYeC as "Proprietary Data;" or
g) any of the foregoing even when categorized under a different name (e.g., a person's social security number used as an account number).

"**Privacy Rule**" means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and subparts A and E of Part 164.
"**Secure Facility**" means the physical location(s) where Proprietary Data can be stored or electronically processed. Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves and the facilities used to support their operation. For the purposes of this agreement, the secure facility will be_____.
"**Security Rule**" means the Security Standards and Implementation Specifications at 45 CFR Part 160 and subparts A and C of Part 164.
"**Services**" means the Services provided by Consultant, Consultant Employees and/or Approved Consultant Resources to NYeC pursuant to the Agreement. For purposes of this Addendum, Services shall include, but not be limited to, Processing as defined herein.

2. Rights and License in and to Proprietary Data

Consultant agrees that as between NYeC and Consultant, all rights including any intellectual property rights in and to Proprietary Data shall remain the exclusive property of NYeC, and Consultant has a limited, nonexclusive license to use this data as provided in the Agreement solely for the purpose of performing its obligations thereunder. Neither the Agreement nor these Requirements provide Consultant any rights, implied or otherwise, to Proprietary Data.

3. Proprietary Data Handling Requirements

When accessing, storing, processing, or transmitting NYeC Proprietary Data or Systems, Consultant shall:

I. Prohibition of Unauthorized Use or Disclosure – Consultant agrees to hold Proprietary Data in strict confidence. Consultant shall not use or disclose Proprietary Data received from or on behalf of NYeC except as permitted by the Agreement or this Addendum, as required by law, or otherwise authorized in writing by NYeC.
II. General Security
    a) process Proprietary Data only in accordance the terms of the applicable agreement between NYeC and Consultant, including, without limitation, these Requirements.

b) maintain and utilize a reasonable privacy and security training program applicable to all Consultant Employees and Approved Consultant Resources that includes, without limitation:
    i. training prior to the commencement of the Services and at least annually thereafter;
    ii. training on the roles and responsibilities of Consultant Employees and Approved Consultant Resources with respect to the security and privacy of Proprietary Data, including incident response training;
    iii. documentation of such training, including content and attendance, which shall be provided to NYeC upon request; and
    iv. providing refresher training from time to time and as appropriate, or as part of discipline/sanctions, for Consultant Employees and Approved Consultant Resources who are not compliant with this Addendum.
c) have in place written confidentiality agreements or obligations with all Consultant Employees and Approved Consultant Resources that are at least as restrictive as those in the Agreement and this Addendum.
d) protect against any anticipated threats or hazards to the security or integrity of Proprietary Data, including, without limitation:
    i. reasonable efforts, through the use of industry standard virus and malware protection software and other customary procedures, to avoid introducing or permitting the introduction of any virus into the NYeC environment; and
    ii. reasonable efforts to regularly check for and delete viruses and malware in the Consultant systems used by consultant to provide the Services by way of standard industry virus and malware detection tools.
e) protect against unauthorized access to or disclosure or use of Proprietary Data which could result in substantial harm or inconvenience to NYeC, including, without limitation:
    i. implementing administrative, technical, and physical security controls to limit access by Consultant Employees and Approved Consultant Resources and NYeC authorized subcontractors to only the minimum amount of Proprietary Data needed to provide the Services in the Agreement
f) implement and maintain security policies, procedures, and programs that meet or exceed National Institute of Standards and Technology (NIST) 800-53 publication, Security and Privacy Controls for Federal Information Systems and Organizations ("NIST Security Standard") and any successor standards thereto.
g) implement business continuity and disaster recovery plans necessary to ensure systems, services, and information are not unavailable for a period in excess of twenty-four (24) hours.
h) implement data breach and incident response policies and procedures.

i) take prompt corrective action(s) to remedy a violation of (and to prevent future violation of) any of these Requirements.

III. Breaches

a) within one business day of a Breach involving NYeC Proprietary Data being suspected and/or confirmed, notify NYeC via email as follows:
   a. Contact the primary contract point of contact; and
   b. NYeC's information security team at infosec@nyehealth.org; and
   c. operationscenter@nyehealth.org

b) take prompt corrective action(s) to remedy a Breach and to prevent future Breach.

c) take prompt corrective action(s) to remediate any vulnerabilities or security concerns in accordance with Consultant's policies and procedures and this Addendum.

d) implement corrective action(s) in a timeframe commensurate with the risk or as agreed upon with NYeC.

e) cooperate fully with NYeC in facilitating investigation and remediation of a Breach.

f) not inform any third party of any Breach except as specifically required by applicable law, without first obtaining NYeC's prior written consent.

g) promptly notify Consultant's primary NYeC business contact of any complaint received related to processing of Proprietary Data.

IV. **Where NYeC has provided written authorization for the** storage/processing/transmission of NYeC Proprietary Data, Consultant shall:

a) if available, provide evidence of a current (within the past 12 months) external security audit such as ISO 27001, SOC 2 Type 2 CMMC, PCI DSS ROC, HITRUST or similar

b) provide for daily back-up of NYeC Proprietary Data and archival of such NYeC Proprietary Data at a secure facility

c) encrypt all Consultant storage devices and networks utilizing industry standard encryption techniques

d) require all Consultant Resources to use only Consultant owned and managed devices to store/process/transmit NYeC Proprietary Data

e) prohibit storage to portable computing devices, e.g., USB drives, cameras and camera phones, and any other portable device that would allow the capturing, printing, or storing of NYeC Proprietary Data

f) establish written procedures for the disposal of electronic storage devices and information, which include the destruction and sanitization of all NYeC Proprietary Data, compliant with NIST 800-88, or a NAID certified 4th party

g) provide industry standard firewalls, both network and device based, that regulate all data entering Consultant's internal data network from any external source, and which will enforce secure connections between internal and external systems and will permit only specific types of data to pass through

h) prohibit the use of NYeC Proprietary Data in Consultant non-production environments
i) implement audit controls that record and monitor systems activity continuously, including logging of who has accessed NYeC Proprietary Data

V. Consultant Provided Software and/or Code
a) not knowingly insert or knowingly allow the insertion into the Software of any code which would have the effect of wrongfully disabling or otherwise wrongfully shutting down all or any portion of the Services.
b) Train Consultant Employees and Approved Consultant Resources in proper techniques for developing secure applications.
c) upon discovery of software and system vulnerabilities, provide software patches to remediate vulnerabilities, based on a severity rating mutually agreed upon by the parties, within seven (7) calendar days for High/Critical vulnerabilities, fifteen (15) days for medium vulnerabilities, and thirty (30) days for Low vulnerabilities.
d) perform application security analysis and testing (also called "verification") according to the verification requirements of an agreed-upon standard (such as the OWASP Application Security Verification Standard (ASVS)). Consultant shall document verification findings according to the reporting requirements of the standard. Consultant shall provide the verification findings to NYeC, at a minimum, annually.
e) where the Services involve the provision of code to be used for NYeC's website, conduct web application security scanning prior to production. If the results of the web application scanning identify any security issues, NYeC reserves the right to require Consultant to correct those issues deemed critical (by NYeC's judgement) by changing the code at no additional cost to NYeC. The timeline for the remediation of such issues will be negotiated by NYeC and Consultant but will not exceed a 60-day remediation period.

4. Consultant Personnel Requirements

Consultant shall ensure that, consistent with all applicable legal requirements (including but not limited to NYS Human Rights Law) a background check is performed on all Consultant Employees and Approved Consultant Resources prior to hiring or otherwise engaging such Consultant Employees and Approved Consultant Resources if they will have access to Proprietary Data that includes, at a minimum, the following:

a) verification of legal authority to work in the United States;
b) review of an individual's currently pending arrests or criminal accusations, and any record of criminal conviction history in all counties in which the individual resided or worked for more than 30 days within the past seven years to ensure personnel have not been convicted of (i) a felony offense within the past seven (7) years related to violent crimes, property

offense, substance abuse, or fraud; or (ii) any misdemeanor related to violent crimes, property offense, substance abuse, or fraud. Criminal conviction history checks include a review of all federal, state, and local criminal conviction records; and

c) verification that no personnel are listed on the Office of Inspector General (OIG) sanction and disqualification list.

For purposes of these guidelines, the term "Criminal Conviction" includes probation, deferred adjudication, and no contest pleas.

5. Connectivity Requirements

Where Consultant is permitted to access any internal NYeC systems, applications, or networks (collectively "**NYeC Systems**"), Consultant shall:

a) only connect to NYeC Systems through the manner and means authorized by NYeC.
b) not connect to, access, attempt to access, or use any NYeC Systems without the prior written authorization of NYeC.
c) notify NYeC when Consultant Employees or Approved Consultant Resources with access to NYeC Systems has left the Consultant or employer, or no longer has need to access NYeC Systems.
d) not use any NYeC System in any way that is illegal, abusive or creates a security risk or vulnerability.

e) Workforce members and third-party users shall be informed that they may not, under any circumstances, attempt to prove a suspected weakness in a system or service.

6. Off-Shore Processing

No NYeC Proprietary Data, including PHI and PII, may be transmitted, accessed, or stored outside of the United States, including storage via server storage, backup, printing, photography, copy, paste or similar functions.

Consultant shall not use a third-party subcontractor or vendor to provide any Services under the Agreement, without NYeC's prior written consent.

7. Certification and Compliance Requirements

These Requirements shall apply to all Proprietary Data which is: (i) Processed by Consultant, (ii) provided to consultant by or on behalf of NYeC, or (iii) learned, accessed, or otherwise used by consultant during or in connection with the performance of Services under the Agreement, or (iv) stored by Consultant.

Further, Consultant shall provide documentary evidence to NYeC to show compliance with the applicable Requirements, upon request of NYeC. Documentary evidence may include, but is not limited to, summaries of the Consultant's applicable security policies and standards, and/or written certifications of Proprietary Data destruction.

8. Compliance with Business Associate Agreement

In the event the Services result in Consultant becoming a Business Associate, as defined in 45 CFR §160.103, or a subcontractor or Business Associate of a Business Associate, Consultant shall be in compliance with the applicable requirements of (i) the Privacy Rule, including but not limited to implementation of appropriate safeguards to protect the privacy and confidentiality of any PII in the possession of Consultant, Consultant Employees and/or Approved Consultant Resources; (ii) the Security Rule, including but not limited to the implementation of appropriate administrative, technical and physical measures to ensure the confidentiality, integrity and availability of any electronic PII and to protect against reasonably anticipated threats, hazards and unauthorized uses or disclosures of any electronic PII in accordance with the standards and implementation specifications under the Security Rule; and (iii) any applicable Business Associate Agreement.

Consultant shall be responsible under this Addendum for any failure of Consultant, Consultant Employees and/or Approved Consultant Resources to comply with the terms of any applicable Business Associate Agreement or the laws referenced therein applicable to Consultant, Consultant Employees and Approved Consultant Resources in the same manner and to the same extent it would be responsible for any failure to comply with its other obligations under this Addendum.

9. Third Party Compliance

Consultant shall be solely responsible and liable for ensuring that all Approved Consultant Resources who Processes NYeC Proprietary Data as part of Consultant's performance under the Agreement fully comply with the provisions of this Agreement, including but not limited to Section 11, Audit Rights.

10. Non-Compliance

Consultant's failure to comply with any Requirement in this Addendum shall constitute a material breach of the Agreement(s) with NYeC. Without limiting any other right or remedy that NYeC may have, NYeC reserves the right to terminate, for default or breach, the Agreement as a result of such non-compliance in accordance with the terms of the Agreement.

11. Audit Rights

To the extent that Consultant stores or maintains Proprietary Data, Consultant shall, upon reasonable notice, allow its data processing facilities, systems, procedures, and documentation to be inspected by NYeC or designee(s) thereof, to assess compliance with these Requirements, any applicable law, and the Agreement between NYeC and Consultant. Consultant shall reasonably cooperate with such audit requests by providing access to personnel, physical premises, documentation, and infrastructure which Consultant uses to perform its obligations under the Agreement.

In the event that any NYeC Proprietary Data is processed or available through a Consultant website, Consultant shall conduct annual penetration tests and vulnerability scans. Within thirty (30) days of the completion of such tests and scans, Consultant must provide the results of such testing and, where deficiencies have been identified, corrective action plans to NYeC upon request.

12. Delegation by NYeC

NYeC may delegate any right granted to NYeC under these Requirements. Consultant shall provide such access, information, data, and cooperation to such designee as consultant is required to provide NYeC under these Requirements.

13. Survival of Requirements

These Requirements shall remain in effect so long as Consultant has any NYeC Proprietary Data, regardless of any termination, amendment, or executions of other agreements, and further shall remain in effect until consultant has certified to the satisfaction of NYeC that all Proprietary Data held by any Consultant Resources has been destroyed or returned to NYeC, in accordance with these Requirements. Where retention of Proprietary Data is required by law, these Requirements shall remain in effect for the period required by applicable law, after which time, Consultant shall certify to the satisfaction of NYeC that all Proprietary Data held by any Consultant Resources has been securely destroyed or returned to NYeC, in accordance with these Requirements.

14. Indemnity

Notwithstanding any provision to the contrary in the Agreement, Consultant shall defend and hold NYeC harmless from all claims, liabilities, damages, or judgements involving a third party, including NYeC's costs and attorney fees, which arise as a result the failure of any Consultant Resources to meet any of its obligations under this Addendum.

15. Amendments

Any and all proposed or actual changes to this Addendum, including, but not limited to, any permitted exceptions to the Requirements herein must be made in writing pursuant to the Agreement.

IN WITNESS WHEREOF, the Parties have each caused these Requirements to be signed and delivered by its duly authorized officer, all as of the date first set forth above. Consultant acknowledges that the Agreement allows access to NYeC Proprietary Data.

☐ All requirements in this document apply

☐ All of the requirements in this document apply, with the *exception* of:

Section 3, Proprietary Data Handling Requirements

☐ Storing/Transmitting NYeC Confidential Information

☐ Provided Software

☐ Section 5, Connectivity Requirements

NYeC	**CONSULTANT**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____