Request for Proposals (RFP) For

NYeC HITRUST ASSESSOR & SECURITY TESTING

ISSUED BY THE

NEW YORK eHEALTH COLLABORATIVE

RFP INFORMATION	
CONTACT NAME	NYeC
EMAIL ADDRESS	HITRUSTRFP@nyehealth.org
SUBMISSION DEADLINE	February 1, 2023

All correspondence and proposals should be submitted via email directly to the email address listed above and include '**NYeC HITRUST ASSESSOR & SECURITY TESTING'** in the subject line.

I. STATEMENT OF PURPOSE

The New York eHealth Collaborative ("NYeC") is seeking applications from experienced vendors to provide HITRUST assessor services for NYeC and to conduct NYeC's annual security testing. The request consists of two parts, and applicants may choose to apply to one or both parts. Applications should include how the firm plans to:

Option A:

- Provide effective and efficient HITRUST assessor services to enable NYeC to maintain its HITRUST certification status.

Option B:

- Conduct NYeC's annual HIPAA Security Risk Assessment, penetration testing and ethical hacking, as required by the New York State Department of Health ("NYS DOH").

II. INTRODUCTION

NYeC is a non-profit organization, working in partnership with the New York State Department of Health to improve healthcare by collaboratively leading, connecting, and integrating Health Information Exchange (HIE) across the state.

NYeC is New York State's designated entity (SDE) who leads the advancement of the Statewide Health Information Network of New York (SHIN-NY), a network connecting healthcare professionals statewide. The SHIN-NY connects all the regional health information organizations (RHIO), or Qualified Entities (QEs), which allow participating healthcare professionals, with patient consent, to quickly access electronic health information and securely exchange data with any other participant. Each QE operates its own network that aggregates data from electronic health records (EHRs) from participating providers in their regions. They are interconnected through a SHIN-NY hub via the statewide patient record lookup (sPRL). The hub is an orchestration and security appliance. Together, the QEs collect and exchange data from acute care hospitals in New York State, provider systems, individual providers, laboratories, public health departments and other data sources such health insurance payers.

III. BACKGROUND INFORMATION

To receive funding from the New York State Department of Health (NYS DOH), NYeC, as a SHIN-NY entity, is required to (1) attain and/or maintain (full and interim) the certification of a third-party health care industry common security framework using certified assessors (referred to hereafter as "HITRUST assessment"), and (2) the following annual assessments: (a) HIPAA

Security Risk Assessment (internal vulnerability, external vulnerability, external network penetration testing); and (b) HIE Platform Risk Assessment ([a] and [b] referred to hereafter collectively as "Security Risk Assessments").

NYeC's HITRUST certification anniversary date is October 22. NYeC will be undergoing a HITRUST interim assessment in 2023 and a full HITRUST assessment in 2024.

IV. ELIGIBILITY CRITERIA

Required skills and qualifications:

- Applicants for Option A of this RFP must demonstrate current, up-to-date certification as a HITRUST CSF External Assessor and experience and expertise in conducting successful HITRUST full and interim assessments for entities in the health information exchange or similar industry.
- Applicants for Option B of this RFP must demonstrate experience and expertise in conducting security audits, security tests and/or security assessments using control and risk assessment frameworks such as HIPAA and NIST SP 800-30.
- Able to complete the New York State Vendor Responsibility Questionnaire;
- The selected vendor will be required to adhere to certain New York State grant contract, confidentiality and other requirements, including security requirements, specific to the initiative. These requirements will be outlined in the vendor contract.

Preferred skills and qualifications:

- Previous experience with assisting clients in achieving HITRUST certification (Option A) and completing security assessments (Option B) using methods and means that efficiently leverage available tools and evidence (e.g., implementing a protocol whereby the assessor applies evidence provided by NYeC to all applicable controls).

V. MANDATORY REQUIREMENTS

All applicants must submit NYeC's Third Party Security Risk Assessment Questionnaire. Please email HITRUSTRFP@nyehealth.org for a copy of NYeC's Third-Party Security Risk Assessment Questionnaire.

VI. SCOPE OF WORK

Applicants should provide NYeC with a proposal that addresses all areas outlined in Section VII. A detailed project plan must be included outlining project timeline, activities, resources, deliverables, budget, and milestones. Proposals must clearly detail the vendor's approach for

submitting NYeC's validated HITRUST assessment by its annual certification expiration date (October 22) and/or completing its Security Risk Assessments within a timeframe that enables NYeC to report out to NYS DOH to meet its contractual deliverables.

For Option A: In 2022, NYeC was assessed on HITRUST CSF Version 9.5.1 and NYS DOH will set the required CSF Version and scope for the 2024 full assessment in late 2023. For reference, the 2022 HITRUST Certification Requirements for NYeC are attached hereto as Appendix A. NYeC expects NYS DOH to issue similar certification and scoping requirements for 2024.

The proposal should describe in detail the specific, consistent resources, methods and processes that will be deployed to accomplish NYeC's HITRUST assessment submission by October 22 of each year.

For Option B: In 2023, the NYS DOH requirements for the Security Risk Assessments are as follows:

HIPAA Assessment

Activity: NYeC will conduct the required annual HIPAA security risk assessment to ensure measures have been taken to reduce the risk to ePHI to prevent data breach. NYeC shall utilize a third-party assessor to:

- Conduct HIPAA internal vulnerability assessment
- Conduct HIPAA external vulnerability assessment
- Conduct HIPAA external network penetration testing (Pentest)

Deliverable: A annual report summarizing findings that includes the following:

- Executive Summary
- Assessment findings in aggregate for SHIN-NY Enterprise broken out by:
    - HIPAA internal vulnerability assessment findings
    - HIPAA external vulnerability assessment findings
    - HIPAA external network penetration testing (Pentest) Assessment Findings
    - Assessment findings including proposed remediation plan and remediation that has occurred since prior year risk assessment
- Conclusion

HIE Platform Assessment

Activity: NYeC will utilize an independent third-party assessor to perform a risk assessment of the HIE platform using a standard risk assessment framework such as NIST SP 800-30 NIST Risk Management.

Deliverable: A final security risk assessment report completed by an independent third-party

assessor of the HIE platform using a standard risk assessment framework NIST SP 800-30 NIST Risk Management. The assessment report shall include but is not limited to: reported cyber security incidents, HIE company's security certifications/evaluations and cadence, cadence of patch/revision/version release(s) for HIE software, current litigation, themes of litigation (e.g., information blocking, data breach, data transformation, etc.), as identified by the third-party assessor.

The report should include:

- Executive Summary
- Assessment findings for the HIE software platform
- Proposed risk mitigation plan
- Conclusion

A summary of the status of all remediation efforts related to findings from prior years' HIE platform assessments shall be included in the third-party assessor's final report or provided separately.

The proposal should describe in detail the specific, consistent resources, methods, and processes to accomplish the required Security Risk Assessment activities by the timelines prescribed in NYeC's contract with NYS DOH. For 2023-2024, those timelines are expected to be as follows:

- HIPAA Assessment – Final report due to NYeC by September 15, 2023
- HIE Platform Assessment – Final report due to NYeC by July 15, 2023
- Validation testing – Results/report due to NYeC by March 31, 2024

VII. CONTENTS OF PROPOSAL

1. **Applicant Overview and Qualifications**

   The proposal should provide a general overview of the applicant's capabilities, resources, and experience. The ideal applicant will have at least five years of HITRUST assessment and/or security risk assessment experience and expert familiarity with all applicable frameworks and standards. Additionally, the applicant must provide samples of assessment roadmaps and reports (redacted as needed) and provide three references of similar projects undertaken in the previous five years to demonstrate background, experience, and expertise in HITRUST assessment and/or security risk assessment.

2. **Approach and Plan**

   The proposal should include a thorough, detailed approach and plan to conduct the HITRUST assessment and/or the Security Risk Assessment.

- The plan must specifically describe in detail the approach proposed to undertake the project, including proposed best practice methods and processes and a description of value-added services provided (e.g., policy and procedure templates, evidence collection tools, tracking and project management tools).
- The plan must include a project outline, including use of tools, approach, timeline, submission, and cadence of reports (including regular progress reports and reports outlining findings, compliance gaps, corrective actions, recommendations), and requirements of NYeC during assessment and any corrective action.

3. Cost

The proposal must include a detailed budget for complete HITRUST assessment services (Option A) and/or Security Risk Assessment services (Option B), including delivery of report(s) with findings, recommendations, and corrective actions, where applicable.

VIII. APPLICATION PROCESS AND TIMELINE

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

Proposal submissions are due no later than **February 1, 2023.** Organizations may only contact NYeC using the email address **HITRUSTRFP@nyehealth.org** for all matters concerning this RFP.

If you have questions about the application, please submit those questions to the designated mailbox noted on the cover page of the RFP by January 4, 2023 by 12 p.m. EST and NYeC will post all questions received and answers to those questions by January 6, 2023 by 5 p.m. EST to https://www.nyehealth.org/rfis-rfps/.

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 in Microsoft Word format using font size 12 with a maximum of 10 pages. Samples of previous work may be included in addition to the 10 pages, though may not exceed three examples. All valid applications must include all sections identified in the evaluation criteria.

Item	Due Date
RFP Release	December 19, 2022
Deadline to submit Questions to NYeC	January 4, 2023, by 12 p.m. EST
Q&A Document posted	January 6, 2023, by 5 p.m. EST
Proposal due	February 1, 2023, by 5 p.m. EST

IX. EVALUATION CRITERIA

All proposals are to address and be evaluated upon the following criteria (10-page maximum proposal length) as it relates to Section VI. Contents of Proposal.

A. Applicant Overview and Qualifications – 30 Points
B. Approach and Plan – 50 Points
C. Cost – 20 Points

SHIN-NY HITRUST CERTIFICATION REQUIREMENTS

- All SHIN-NY entities shall be HITRUST Certified on latest CSF version available (v 9.5.1 or higher)
- Certification must be obtained by certification expiration date or no later than 12/31/2022
- Must use a certified HITRUST assessor and submit evidence to DOH prior to 2022 certification activities commencing
- Must complete a validated assessment including only controls required for certification
- All entities applying for certification shall adhere to the HITRUST SCOPE REQUIREMENTS
- All entities shall submit a HITRUST Scope Attestation to include:
  - Data flow diagram
  - Scope output from MyCSF
- Bi-monthly meetings with NYS DOH and NYeC

HITRUST SCOPE REQUIREMENTS

- To ensure that the required critical security controls are in place and comply with State and Federal laws and regulations an organization's scope for a HITRUST CSF validated assessment with certification must include:
  - Any application or hardware that will transmit, store, process, or permit access to PHI including Department MCD, whether locally hosted and or in the cloud;
  - Any location from which individuals will access PHI including MCD, or provide local or remote system support; and
  - Any device used to access or support the system; including, but not limited to, tablets, desktops, and laptops.
- Organization Type: Health Information Exchange
- Entity Type: Business Associate
- Regulatory Factors: Subject to NY OHIP Moderate-Plus Security Baseline Requirements
- Controls Required: Only Controls Required for Certification

DOH Guidance

- The Department requires organizations to provide detailed comments explaining how organizational controls satisfy each HITRUST Requirement Statement in the comments section of the HITRUST report.
- An organization that believes that a certain security control or control requirement is "Not Applicable", or "N/A", must provide specific reasons why there is an exception.

NEW YORK STATE OF OPPORTUNITY. Department of Health