Request for Proposals (RFP) for
NYeC HITRUST Assessor & Security Testing

Questions & Answers

1. Will the scope be the same for the HITRUST, HIPAA, and Systems Assessment Report (e.g., systems, data types, integrations, facilities / locations)?
   - If yes, please describe the systems and environments and facilities in scope?

   Response: Systems in scope include Statewide Patient Record Lookup (sPRL), Corporate Network, and NYeC-managed cloud resources in AWS.

   - If no, please provide a detailed description of the systems, environments, and facilities in scope for each assessment:
     1. HITRUST
     2. HIPAA
     3. (Systems Assessment Report)

2. Can you describe the preferred criteria for conducting the SHIN-NY Systems Assessment Report (e.g., standards, frameworks)?

   Response: NIST SP 800-30 Guide for Conducting Risk Assessments is the required framework for the SHIN-NY Systems Assessment.

3. HIPAA Internal Network Penetration Testing - how many live IP addresses (hosts) are in scope?

   Response: Up to 200 internal IP/hosts
   - Servers (Physical and/or Virtual) <50
   - Workstations and Laptops (Physical and/or Virtual) = n/a
   - Network Devices (including Wireless Access Points) = <20
   - Printers and Multi-Function Devices = <5
   - IoT Devices (cameras, sensors, badge systems, alarms, etc.) = <30

4. How many unauthenticated web applications are in scope?

   Response: up to 5 applications are in scope; least one is unauthenticated.

5. For the internal penetration test, do you prefer Black-box, Grey/White-box, or both:
   - Black-box: No credentials provided; testing limited to basic network connectivity.

- Grey/White-box: Provide standard user credentials and basic access to simulate an assumed breach (privilege escalation, data exfiltration, etc.). Note: Grey/White-box requires more effort and cost than black-box.

  Response: Grey/White-box is preferred.

6. Would you like social engineering attacks (e.g., phishing simulations)?
   - If yes, how many targets (e.g., 50 admin users + 500 standard users = 550 total)?
   - How many campaigns (distinct exercises/templates)?

   Response: Out of scope.

7. Does the scope of testing include testing cloud service integrations/endpoints (Azure, AWS, etc.) within the internal network? If yes, please provide details on IPs, gateways, firewalls, VPNs, applications, and their purpose.

   Response: Out of Scope, only AWS cloud is used.

8. Would you like to include a 30-day retest option? This allows remediation, validation and report updates. Note: Additional cost applies but it is minimal compared to overall testing

   Response : Yes

9. HIPAA External Network Penetration Testing - How many live IP addresses and/or fully qualified domain names (FQDNs) are in scope?

   Response: Up to 20 external IP addresses/hosts.

10. What is the total number of publicly facing IP addresses (servers, endpoints, web addresses, network devices, etc.)?

    Response: Up to 20 external IP addresses/hosts

11. How many network devices (firewalls, routers, etc.) are in scope?

    Response: Cloud network controls are implemented via AWS services.
    Up to 15 hardware network devices in Office locations.

12. How many unauthenticated web applications are in scope?

Response: up to 5 applications are in scope; least one is unauthenticated.

13. Should our team exploit identified vulnerabilities and perform post-exploitation to demonstrate potential impact?

    Response: No

14. Would you like to include a 30-day retest option? This allows remediation validation and report updates. Note: Additional cost applies but it is minimal compared to overall testing.

    Response: Yes

15. The RFP states: 'Reports must include evidence that OWASP Top Ten was considered in all vulnerability and penetration testing.' Please clarify:

    While OWASP Top Ten may have limited relevance within an internal network pen test (Ex: If the internal network hosts web portals, intranet apps, or APIs, etc..), OWASP Top Ten is primarily focused on web application security risks; consequently, it is mostly relevant when an organization is testing the security of its web applications.

    Hence, If NYeC requires dedicated web application testing aligned with OWASP Top Ten or ASVS Levels 1–3, this will need to be added as an RFP addendum with separate scoping questions. Please indicate whether NYeC requires web application/application penetration testing and/or code reviews for specific applications within the environment in addition to internal and external infrastructure/network penetration testing.

    Response: No code review is required. NYeC requires web application/application penetration testing only.

16. When did NYeC first become HITRUST certified?

    Response: 2018

17. Is the NYeC using any tools to facilitate HITRUST compliance efforts such as Vanta or Drata?

    Response: No

18. Is there a preference between remote or onsite procedures for any of the scope areas?

    Response: There is no preference.

19. Should we include the Third-Party Security Risk Assessment Questionnaire with our proposal submission?

    Response: Yes, please.

HITRUST

20. Please describe scope of the system(s) in-scope for the assessment.

    Response:
    SPRL :
    The sPRL process supports the organization's key strategic goals to increase interoperability across healthcare systems in New York State. These functions act as an integrated, highly secure search engine, allowing participants to retrieve individual patient records from across the state after receiving consent from the patient. To achieve the interoperability goals, the organization has implemented the Health Level 7 standards (HL7 Standards Product Brief - HL7 Version 3: Reference Information Model (RIM) | HL7 International, 2013) and Integrated Healthcare Enterprise profiles such as cross-community patient discovery, cross-community document discovery, and cross-community document retrieval. This process helps authorized, consented physicians retrieve patients' clinical data for treatment purposes. The patient discovery process helps to search for a patient across the network to locate where they have clinical data that physicians can use for their current and future treatment. A central repository has been built to store patient identification information to achieve this. This repository is also known as the Master Patient Index, and all other organizations connect to it for feeding and query the patient's treatment location to pull the data for their current and future treatment.

    Snowflake:
    NYeC uses Snowflake as the data analytics tool. Its a HITRUST compliant platform. NYeC has implemented SSO integration to its existing identity tool, Azure AD, and inherited all security controls from its existing HITRUST certified policies and procedures to ensure the security posture of the Snowflake environment. After data is received by the DATA LAKE, the data is read and validated before being processed and prepared for Snowflake data ingestion via managed workflows. Once the data has been read and processed, the workflow triggers Snowflake's ingestion of the data, where further ETL operations are performed to create the query-able golden

record outputs. While the use of Snowflake is managed by NYeC Data Lake Engineers and it runs on AWS, the Snowflake platform is hosted by Snowflake.

Data Lake:
The SHIN-NY Data Lake Project (AKA Public Health Data Lake or Data Lake) establishes a centralized, cloud-based repository for statewide data, including clinical data from the six Qualified Entities (QEs), in New York State (NYS). The overall goal of the system is to support the NYS Department of Health (NYSDOH) in public health and Medicaid activities, for approved use cases as well as serve as the central repository for social determinant of health screening and referral data that will be collected as part of the 1115 Medicaid waiver implementation. In addition, should NYeC receive Medicaid Confidential Data (MCD) from DOH in the future, that data would also be stored in the Data Lake in accordance with the applicable Data Use Agreement (DUA) and requirements. NYeC would apply, at a minimum, the same level of privacy and security safeguards to protect MCD within the data lake as are described in this document for PHI/PII; NYeC would implement the same HITRUST-approved policies and procedures with respect to any MCD received in the future as are described herein. At this time, the system's primary elements are data ingestion from QEs. Data processing and storage is in AWS, and data ingestion into Snowflake, resulting in readily query-able data to help support the NYSDOH. For the monitoring and observability of the AWS and Snowflake environments, Datadog is used for AWS logs. The DATA LAKE system ingests, processes, and stores MPI, historical data as well as real-time Fast Healthcare Interoperability Resources (FHIR) data. Data is sent to the DATA LAKE via SFTP file transfer systems and utilizing REST API posting of data via HTTPS connection. Key protections for the data ingestion components of the system include restricted IP connectivity via whitelisting, separate credentials for each data type, QE, and environment, least privilege permissions for QEs connecting to the data transfer points, and encryption at-rest (AES-256) and in-transit (SSL).

21. Please provide an overview of the corrective actions that will require follow-up from the previous audit.

    Response: NYeC will only disclose that information after contract is signed.

22. Was HIPAA included in the scoping factor of the last validated assessment and is there a consideration to add it to the i1 assessment?

    Response: Original R2 assessment included Office of Health Insurance Programs (OHIP) related controls. OHIP controls will not be added to i1 as DOH moved that assessment to SSP workbooks.

23. Under III. Background information, there is a mention of maintaining full and interim certification, this implies an r2 assessment, just confirming this proposal needs an i1 assessment.

Response: Proposal needs only i1 assessments.

24. Are all aspects of SHIN-NY locally hosted or cloud based in order to determine if external inheritance is needed?

    Response: Cloud based only, AWS.

25. Will there be a dedicated resource to facilitate evidence gathering to ensure all HITRUST test procedures are submitted within the 90-day timing?

    Response: Evidence gathering is conducted by internal team, that includes SME's, security team and depending on scope, a project manager.

26. Will we need to leverage the work of internal assessors or will the external assessor be responsible for all validated testing?

    Response: External assessor will be responsible for all validated testing.

27. Please confirm – while previously a r2 assessment was performed, you are transitioning to the i1 for 2026?

    a. With the i1, are you selecting any optional compliance factors? If yes, which?

       Response: We are transitioning to i1 with no compliance factors.

28. Can you provide scoping details:

    a. # of Systems / Applications

    Response: See #20

    b. # of Facilities / Type

       Response: AWS cloud

    c. # of Outsourced Services

       1. Are cloud-hosted environments in scope (AWS, Azure, GCP)? If yes, which?

          Response: AWS

    d. Planned Inheritance (full vs partial)

          Response: Max acceptable by HITRUST.

    e. Approximate number of users across in-scope systems

       Response: Less than 100.

29. Are control processes standardized across all in-scope systems?

    Response: Yes

30. Approximately how many subject matter experts / control owners will participate in interviews?

    Response: up to 10

31. Does NYeC utilize any GRC platforms the auditor will be interfacing with?

    Response: No

32. Can we get the following HITRUST scoping items from the most recent r2 (or a copy of the previous report):

    - Are measure and managed in scope? No
    - Is Privacy in scope? No
    - Number of locations? AWS
    - Number of employees? <50
    - Number (and names) of in scope services and platforms? See #20
    - Regulatory factors to be included in scope? I1 only.

HIPAA

33. HIPAA-Please describe the detailed scope of the NYeC entities that are to be included in this assessment.

    Response : NYeC and subcontractors only (<10).

    A. Please identify the locations, platforms, systems, application, APIs, and PHI data sets that are in scope.

       Response: Please see #20.

34. NYeC appears to refer to the HIPAA Compliance Review and HIPAA Security Risk Assessment as if they are synonymous and part of the same review/assessment.

    A. Is this an accurate statement?

    Response: The efforts can be largely re-used, but are distinct. DOH guidance requires compliance review, internal/external vulnerability assessments, internal/external pen tests, with a formal HIPAA Security Risk Assessment using NIST SP 800-30 and OWASP, plus POA&M per FedRAMP. Compliance review feeds the RA and POA&M; RA is the formal risk analysis/report.

B. If not, please clarify NYeC's expectations and outcomes for the HIPAA Compliance Review and the HIPAA Security Risk Assessment.

Response: See A

C. If applicable, for the HIPAA Compliance Review, please describe the requirements.

Response: See A

- What are the HIPAA Rules and Standards that the review should measured compliance against?

Response: 45 CFR Part 164, Subpart C , NIST SP 800-30 / 800-53

- Please provide the references to the HIPAA Rules and Standards.

Response: 45 CFR Part 164, Subpart C

35. Part 1 of Deliverable 1.5.17 stated that the Assessor should "complete the HIPAA Risk Assessment conducted by the Security Risk Assessment Tool (ASTP Security Risk Tool). Please confirm whether:

A. The Assessor is responsible for reviewing and validating the completed copy of Security Risk Assessment prepared by NYeC, or

B. If the Assessor is responsible for completing the Security Risk Assessment tool? If so, please describe the desired format for the SRA tool deliverable (Windows, Excel, etc.).

Response: Assessor is responsible; Excel is acceptable.

36. Are the HIPAA Compliance Review and/or HIPAA Security Risk Assessment required to be performed onsite at the in-scope locations?

A. If yes, please identify the number of locations and the expected duration for each onsite review.

Response: No onsite review is required.

External Network Penetration Testing

37. Is the external perimeter part of the assessment?

    Response: Yes

    a. If so, how many unique external IP addresses will be part of the scope?

       Response: Under 20

    b. Will phishing be part of the assessment?

       Response: No

38. Are there any externally accessible services (e.g., VPN, portals, admin interfaces) requiring deeper testing?

    Response: Same standard applies to all application testing.

39. Please provide all the domains to be tested.

    Response: Details will be provided after project kickoff.

40. Would you like any web applications included as part of external network testing?

    □ Yes

    □ No

    Response: Yes

41. If yes, please list each application:

Application Name	URL	External / Internal	Authentication Required?	Number of User Roles	Contains PHI?
		External / Internal	Yes / No		Yes / No

Response: Details will be provided after project kickoff.

Internal Network Penetration Testing

42. Is the internal network part of the assessment? Yes

43. Approximate number of internal IPs/systems in scope: _____ up to 200_____

44. Number of subnets/VLANs to be assessed: ____under 10______

45. Please provide the total number of servers? Approximate count: ____under 50_____

46. How many web applications are part of the assessment?

    a. Will authenticated testing be performed?

        Response: Yes

        1. If so, how many roles will be tested?

        Response: Max 2

    b. How many API endpoints will be part of the assessment?

    Response: Under 10

47. Is your network on-premise (traditional), in the cloud e.g. Azure, AWS or hybrid?

    Response: AWS

48. Is the internal network accessible from a single logical location for testing? If not, will your team be able to move the testing device between network segments as needed, or will multiple devices be required?

    Response: Both options are available.

49. If multiple devices are needed, please indicate how many and which segments they should be placed in.

    Response: One with access to DEV, QA, PROD segments, or one in each.

50. What authentication details or test accounts will be provided for penetration testing?

    Response: AD account and authentication.

51. Are there custom applications or third-party integrations that require deeper OWASP-based testing?

    Response: To ensure strong Advanced Programming Interface (API) security, the Open Web Application Security Project (OWASP) Top Ten will be incorporated into all vulnerability and penetration testing.

Are there specific timeframes where vulnerability and penetration testing can be performed? Does testing need to take place outside of business hours?

Response: There is no time constraint; only non-destructive pen testing is allowed.

Vulnerability Assessments

52. Preferred scan type:

☐ Credentialed (recommended)

☐ Uncredentialed

Response: Credentialed when possible.

53. Do you have internal vulnerability scan results you would like us to compare against?

☐ Yes

☐ No

Response: No

API Security Testing

54. Would you like API testing included?

☐ Yes

☐ No

Response: Yes, detailed information will be provided after the project kickoff.

If yes, please provide:

☐ API Documentation (Swagger / Postman)

Authentication Type: ________________________________

Number of Endpoints: __________

External or Internal? External / Internal

Processes PHI? Yes / No

Cloud Environment (If Applicable)

55. Do you use any cloud platforms? AWS / Azure / GCP / Other: __________

    Response: AWS

56. Would you like a cloud configuration/security review? If yes, then please provide additional details

    Response: No

57. Are cloud resources connected to SHINNY or PHI systems? Yes / No

    Response: Yes

58. Will NYeC provide a finalized inventory or total count of all systems, applications, networks, APIs, and environments in scope for the assessments, including cloud, on-premises, and hybrid systems?

    Response: Yes

59. Any medical devices, EMR/EHR, PACS, or clinical systems requiring restricted testing?

    Response: No

60. For the SHIN-NY Security Risk Assessment, please describe scope of the system(s) in-scope for the assessment.

    Response: See #20