RFP Number: 038-0027
Date: August 21, 2018

Request for Proposals

for

Risk Analysis and Security Assessment Services

All communication regarding this RFP must be to:

Mitchell Jacobs
Director, Supply Chain Services
jacobsm1@nychhc.org

I. RFP Timeline

Date	Action
8/21/2018	Publish RFP
8/28/2018	Mandatory pre-proposal conference: Conference Call
8/31/2018	Proposer questions by 3:00 p.m.
9/14/2018	Submission deadline by 3:00 p.m.

II. NYC Health + Hospitals

New York City Health and Hospitals Corporation ("NYC Health + Hospitals" or the "System") is an integrated health care system of hospitals, neighborhood health centers, long-term care, nursing homes and home care – the public safety net health care system of New York City. NYC Health + Hospitals is committed to the health and well-being of all New Yorkers and we offer a wide range of high quality and affordable health care services to keep our patients healthy and to address the needs of New York City's diverse populations.

About NYC Health + Hospitals - http://www.nychealthandhospitals.org/about-nyc-health-hospitals/

III. Project Description

NYC Health + Hospitals is looking for a vendor to provide annual information risk analysis and security assessment services for all of its facilities, entities, units, programs, and data centers, with a focus on electronic sensitive data including but not limited to electronic Protected Health Information ("ePHI") as defined by the implementing regulations of the Health Insurance Portability and Accountability Act ("HIPAA") of 1996.

The requested risk analysis and security assessment services are broken down into the following seven activities:

1. HIPAA Enterprise-wide Risk Analysis (Application & ePHI Focused)
2. HIPAA Compliance Assessment, including the OCR Audit Protocol
3. Management Plan for addressing identified risks
4. Application Security - Penetration Testing
5. Infrastructure Security - Internal Penetration Testing (including server)
6. Infrastructure Security - Perimeter/DMZ Penetration Testing
7. Vendor Risk Assessment

Further details regarding the seven activities above are discussed in *Section V. Scope of Work.*

IV. Minimum Criteria

The vendor must possess the following minimum qualifications in order to participate in this RFP:

- Firm must have performed risk analysis and security assessment services at a minimum of two health care providers;
- Prior working experience in a hospital or Health Care institution within the past 3 years;
- Must hold, in good standing, HITRUST or other equivalent certification.

Please provide confirmation and supporting documentation that you meet each of these minimum criteria.

V. Scope of Work: Risk Analysis and Security Assessment Services

The statements in this section cover the scope required to fulfill the System's HIPAA and Security Risk Assessment program. The vendor must outline the methodology to be utilized for the enterprise-wide risk analysis and security assessment services, and management plan as described below.

Note that for each of the activities (1 – 7) below, the following statements should also be applied:

- Reports for each activity (1 – 7) must be provided and include detailed findings and recommendations – essentially, technical and executive reports per location, *including separate Meaningful Use reports for Attestation*, as well as an enterprise-wide risk analysis report, and a risk management plan for NYC Health + Hospitals – in PDF and Word formats. Reports should cover the project scope, executive summary, confirmation status of each information security control with recommendations for improvement, and an overall management plan designed to address the identified risks.

- All activities/results must be mapped to HITRUST MyCSF, NIST Controls & NIST Cyber Security Framework, and OWASP Top 10 Application Security Risks (where applicable for applications).

- A baseline must be created so that future analyses/assessments can measure deviations from the baseline, and compare NYC Health + Hospitals with health care industry averages.

1. **HIPAA Enterprise-wide Risk Analysis (Application & ePHI Focused)** - Conduct an enterprise-wide risk analysis, management, and evaluation to meet HIPAA Security Rule §§ 164.308(a)(1)(ii)(A) & (B) and 164.308(a)(8) requirements across the entire NYC Health + Hospitals system, including hospitals, clinics, corporate offices (including subsidiaries), data centers, and MetroPlus - i.e. conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and

availability of electronic protected health information ("ePHI") created, received, maintained, stored, or transmitted by NYC Health + Hospitals, identify security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level, and conduct a technical and nontechnical evaluation, based upon the standards implemented under the Security Rule, in response to environmental or operational changes affecting the security of ePHI. The risk analysis should include ePHI in all forms of electronic media, regardless of the medium in which it is created, received, maintained, stored or transmitted, or the source or location of the ePHI, and should track the movement of such ePHI within the System. Additionally the risk analysis must meet all Meaningful Use/HITECH risk analysis requirements. This activity should be application-focused, and the results must include prioritized risks to all electronic sensitive data especially ePHI that is created, received, maintained, stored, transmitted or processed by the applications, infrastructure (network, workstation, server, web, database, mobile devices etc.) and users. Such risk analysis will include an assessment of threats to the ePHI and the vulnerabilities present in the systems or hardware that create, receive, store, maintain, process or transmit ePHI.

The risk analyses must be in line with NIST guidelines including but not limited to NIST SP 800-66, NIST SP 800-30, NIST SP 800-53 and other guidance available from the U.S. Health & Human Services Office for Civil Rights ("OCR") such as: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

In addition, the Meaningful Use security risk analysis should be performed in accordance with the requirements in 45 CFR § 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created, received, transmitted, or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR § 164.312(a)(2)(iv) and 45 CFR § 164.306(d)(3). Separate security risk analysis reports are required for Eligible Hospitals (Acute Care Facilities) and Eligible Providers (Diagnostics and Treatment Centers). The vendor is expected to stay up to date on Merit-Based Incentive Systems ("MIPS") Advancing Care Information measures.

2. **HIPAA Compliance Validation Assessment including the OCR Audit Protocol** - Perform on-site assessments of all NYC Health + Hospitals locations, including hospitals, clinics, corporate offices (including subsidiaries), data centers, and MetroPlus, each year to ensure the System's compliance with the Privacy, Security, and Breach Notification Rules, and all sub-elements such as HITECH additions, the

Omnibus Rule, and the OCR audit protocol – see, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.

Review existing privacy and security policies and procedures from a HIPAA and best practices standpoint and provide recommendations where deficiencies are found.

3. **Management Plan for addressing identified risks** – Develop a comprehensive management plan that addresses all the risks identified in the enterprise-wide risk analysis, and how to mitigate them. The plan should rank the risks according to their criticality.

4. **Application Vulnerability Assessment - Penetration Testing** - A thorough penetration assessment of 25 enterprise applications per year **(client server and web based)** to uncover all vulnerabilities associated with the applications and supporting infrastructure (endpoints, workstations, servers, network), and highlight the applications that are readily exploitable, along with evidence of vulnerability actually being exploited during testing. This exercise must also identify vulnerabilities which are not possible to detect using automated vulnerability scanning activity. The results must include an application specific threat model (reference Microsoft threat modeling).

   The risk analysis must be in line with HIPAA Security Rule, NIST guidelines including but not limited to NIST SP 800-30, NIST SP 800-53 and other guidance available from OCR guidance on risk analysis.

5. **Infrastructure Security - Internal Penetration Testing (including server)** - A penetration testing of all IP addressable endpoints (or a sample size of at least 10%) including but not limited to workstations, servers, peripheral devices, wireless devices/access points and network/security devices. There are approximately 60K IP addressable endpoints out of which 50K are workstations/laptops. The testing must simulate each phase of the attack lifecycle, identify gaps in the detective control agents, and gather logging and alerting evidence to prove successful or unsuccessful detection.

The workstations operating system is primarily Windows 7 and Windows 10 with a handful of Windows XP, and the network devices are primarily Cisco.

There are a total of 4000 servers with the following operating systems: Windows 2008, Windows 2012, Windows 2016, AIX, Linux.

This must be in line with Open Web Application Security Project (OWASP) and NIST guidelines including but not limited to NIST SP 800-53.

6. **Infrastructure Security - Perimeter/DMZ Penetration Testing** - A thorough penetration testing of all servers to uncover all vulnerabilities and highlight the ones that are readily exploitable, along with evidence of vulnerability actually being exploited during testing. This exercise must also identify vulnerabilities which are not possible to detect using automated vulnerability scanning activity. There are a total of 4,000 servers with the following operating systems: Windows 2008, Windows 2012, Windows 2016, AIX, and Linux. The testing must simulate each phase of the attack lifecycle, identify gaps in the detective control agents, and gather logging and alerting evidence to prove successful or unsuccessful detection.

   This must be in line with Open Web Application Security Project (OWASP) and NIST guidelines including but not limited to NIST SP 800-53.

7. **Vendor Risk Assessment** - Conduct a thorough and detailed risk analysis and security assessment of the System's vendors that are Business Associates of the System. The assessment should provide assurance to NYC Health + Hospitals that the vendor is in compliance with HIPAA, and that the vendor's security controls are in line with NIST and the System's security controls. The assessment should also include assisting NYC Health + Hospitals development of a Vendor Risk Management program.

Supplemental Requirements

- The vendor must be able to demonstrate the following capabilities: Ability to employ an assessment approach that leverages the:

    - OCR Audit Protocol
    - Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
    - Meaningful Use
    - NIST SP 800-53
    - NIST 800-30 and
    - NIST 800-66;

- Ability to provide detail and clarity to the HIPAA Security, Privacy and Breach Notification Rules as well as organizational factors such as type and size/complexity for each control and functional area;

- Experienced assessment team with each member delivering service to NYC Health + Hospitals having a certification (in at least one of the following): HITRUST, CISSP, CISA, CISM, SANS GIAC;

- Provide all assessment Findings and Recommendations in a format (*example: .csv, .xls*) that can be imported into a GRC Tool;

- Provide competitive pricing for on-site assessment review of facilities including but not limited to: 11 hospitals, 5 long term care facilities, 5 diagnostic and treatment centers, 70+ clinics, and 4 Corporate locations, including 2 data centers; and

- Assign a qualified project manager for the term of the engagement.

<u>In regards to this Scope of Work, each responding vendor is expected to provide the following information for evaluation</u>:

1. (Required) Fill column C, D, E and F on tab 1 (Requirements) of the attached spreadsheet.
2. (Required) Provide detailed methodology for each of the 7 assessment activities above as a separate document, along with sample reports for each of the 7 activities identified in the Scope of Work. Methodologies must include what steps will be taken to collect the information, identify threats and vulnerabilities, assess current security measures, determine threat likelihood, impact of threat occurrence, and the level of risk including any tools or technologies that will be used for the risk analysis.
3. (Preferred) Highlight in a separate document any experience dealing with the OCR and/or U.S. Department of Health and Human Services with regard to HIPAA security rule compliance and/or responding to queries and/or audits.
4. (Optional) Highlight any additional related offerings on tab 2 (Additional Offerings) of the attached spreadsheet.

VI. Scoring Criteria

The scoring criteria for the Scope of Work shall be as follows:

Category	Weight %
HIPAA Assessment Experience	20
Security Risk Assessment Experience	25
Assessment Methodology	20
Report Samples	10
Key Personnel/Management	15
Cost to Value	10

VII. Contract and Payment

The term of the contract resulting from this RFP shall be for a period of 2 Years with a potential 1 year extension.

Payment will be net 90.

VIII. RFP Process and Rules of Participation

A. RFP Process

1. Questions. Substantive questions regarding the Scope of Work must be received by the date and time in the RFP Timeline, and by the person designated on the first page of this RFP. Questions not timely received by such person are not guaranteed a response.

2. Conference. A pre-proposal conference is mandatory and shall be held via a conference call at the time set forth in the RFP Timeline.

3. Submission. Proposers shall submit the Proposal Package in digital format on a CD or flash drive by the time and date set forth in the RFP Timeline.

The Proposal Package envelope must include the RFP name and number.

Proposers may submit the Proposal Package in person or otherwise shall use a common carrier with signature and time stamp required.

Proposals that are late or unsealed will not be considered; however, NYC Health + Hospitals may accept late proposals when it is in its best interests and the lateness of the proposal is deemed non-material.

B. Proposal Package Contents

1. Page limit. The Proposal Package shall not exceed 25 pages, not including the Executive Summary, exhibits or other attachments.

2. Cover Sheet. A cover sheet containing the following information must be submitted with the proposal:

RFP Title
Vendor Name and Address
Principal contact person name and contact information
Number of addenda received

3. Table of Contents. The proposer must provide a table of contents with page numbers.

4. Executive Summary. Provide a summary of no more than one page describing how you will meet the goals of the RFP and the cost information.

5. Vendor's Background and Organization: In this section provide the following information:

Number of employees
Organization chart
Audited financial statement for the last 3 years
Background of principals
Recently completed similar size projects
A copy of any licenses relevant to this project
Duration you have been doing business in this service or product line

6. References. List of five current clients and contacts, including email addresses and phone numbers, at least two of which are health care providers.

7. Technical Proposal. The Technical Proposal must address all issues in the Scope of Work and include any other information you believe would be relevant.

8. Cost Proposal. If not already addressed in the Technical Proposal, vendor must set forth a cost proposal including line item detail of equipment, labor and all overhead and profit within the proposal.

9. MWBE Utilization Plan (form attached). NYC Health + Hospitals follows New York State Executive Law Article 15-A which requires 30% participation of New York State Certified MWBEs as subcontractors. The directory of New York State Certified MWBEs can be viewed at: http://bitly.com/1b7OmNI. A MWBE Utilization Plan shall be submitted with the names of the MWBE subcontractors the proposer plans to use to meet such goal. Waivers will only be given after good faith efforts to comply have been demonstrated.

10. NYC Health + Hospitals Terms and Conditions, Form 110-96 (attached). NYC Health + Hospitals does not accept any changes to the terms and conditions set forth as mandatory within Form 110-96. Any exceptions taken to such mandatory terms may result in rejection of the proposal.

Any exceptions to the terms and conditions must be set forth in writing, with reasons for such objection, and alternate language suggested, or are otherwise waived.

11. Confidential or Proprietary Information. NYC Health + Hospitals is a public entity subject to New York State's Freedom of Information Law ("FOIL"). Therefore, any confidential or proprietary information should be marked accordingly to assist in any FOIL request. Such information deemed by the vendor to be confidential or proprietary shall be easily separable from the non-confidential or non-proprietary sections of the proposal.

12. Doing Business Data Form ("DBDF") (attached). In accordance with New York City Local Law 34 of 2007, the proposer must submit an accurate and complete DBDF, enclosed in a separate envelope. Failure to do so will result in rejection of the proposal.

13. Business Associate Agreement ("BAA") (attached). The selected vendor must submit a signed copy of the BAA. No modifications may be made to the BAA.

14. Additional Required Forms. Supply and Service Employment Report, W-9.

C. Rules of Participation

1. Communication with NYC Health + Hospitals. From the date this RFP is issued until the award of contract, proposer and its staff shall direct all communications relating to this RFP solely to the person set forth on the first page of this RFP.

2. Solely within its discretion, the System may withdraw this RFP prior to award of a contract, postpone this RFP, reject all proposals, or choose not to award a contract as a result of this RFP.

3. Addenda. NYC Health + Hospitals may issue addenda to this RFP to correct or clarify the solicitation. It is the proposer's responsibility to ensure that it has received all addenda. Prior to submitting the Proposal Package the proposer should check with the contact person on the first age of this RFP.

4. Modifying Proposals. A proposer may submit a modified proposal to replace all or any portion of a previously submitted proposal up until the submission deadline.

5. Mistakes. NYC Health + Hospitals may waive or modify any mistakes in proposals that are deemed to be not material.

6. NYC Health + Hospitals shall not be bound by any oral or written representations, statements or explanations other than those made in this RFP or in formal written addenda issued to this RFP.

7. Proposal. The proposal is a written offer and shall be irrevocable for six months. The offer may not be withdrawn after the submission deadline.

8. Modifications to or withdrawals of a proposal after the submission deadline shall not be considered.

9. Costs. NYC Health + Hospitals shall not be liable for any costs incurred by proposers in the preparation of proposals or for any work performed in connection therewith.

10. Negotiations. NYC Health + Hospitals may award a contract on the basis of initial offers received. The Proposal Package should therefore contain the proposer's best terms from a programmatic and cost standpoint. NYC Health + Hospitals may choose

to negotiate all proposers or a limited pool of proposers and award a contract to one or more proposers.

11. Award. If a contract results from this RFP the contract will be awarded to the highest-rated responsible proposer(s) based on the evaluation factors set forth in the RFP.

12. Conditions of Award. All proposed awards will be subject to compliance with the System's legal requirements, vendor responsibility determination, and approval by its internal governing bodies.

D. Evaluation

1. Evaluation Committee. An Evaluation Committee shall be formed and comprised of a minimum of five persons who will evaluate the proposals.

2. Scoring. The Evaluation Committee shall score and weight responsive proposals of proposers that meet the Minimum Qualifications in accordance with the scoring criteria set forth above in this RFP.

3. Presentations. The Evaluation Committee may require all or a short list of proposers to give one or more oral or visual presentations in support of their proposals and/or otherwise demonstrate the information contained therein.

Proposal Package Checklist

An envelope addressed to the person set forth on the first page of this RFP, including the name and number of this RFP.	
A flash drive or CD containing the Proposal Package	
Acknowledgment of Addenda, if any	
Doing Business Data Form	
Business Associate Agreement	
MWBE Utilization Plan	
Supply and Service Employment Report	
W-9 Form	
Online Disclosure Filing Vendors must complete an online disclosure filing via the PASSPort system (formerly known as Vendex). 1) Go to: https://passport.cityofnewyork.us. 2) Create a username using your email address. 3) Login with your username and create an account for your company. 4) Complete and submit the online questionnaire.	