



**HIPAA Privacy & Security Assessment
No. ITS-001-26**

**Administration
Information & Technology Service
07/25/2025**

TABLE OF CONTENTS

Table of Contents	2
Introduction	3
Proposal Schedule	4
Application Requirements	4
How to Apply	5
Scope of Professional Services Required	7
Proposal Requirements	13
Statement of Rights	15
Submission Package Checklist	19
Applicant Information – Proposer Cover Page	20

I. INTRODUCTION

The Boston Public Health Commission (BPHC) is an independent agency that provides accessible community-based health services including education, emergency medical services, and resources that contribute to promoting health equity.

To uphold the organization's mission and ensure the confidentiality, integrity, and availability of Information systems, and client protected health information (PHI), BPHC is seeking proposals from experienced and qualified organizations to perform a comprehensive Information Security and HIPAA Risk Assessment that is fully aligned with industry standard security frameworks and HIPAA Privacy and Security Rules.

Proposers interested in providing the HIPAA Privacy & Security Risk Assessment services are invited to respond to this request. It is the BPHC's intent to select Proposer(s) that provide the best solution for the BPHC's needs.

The BPHC reserves the right to amend this RFP. The BPHC reserves the right to reject any or all of the proposals, or any part thereof, submitted in response to this RFP, and reserves the right to waive formalities, if such action is deemed to be in the best interest of the BPHC. The BPHC reserves the right to request additional information from any Proposer. While it is expected that a single award will result for this RFP solicitation, the BPHC reserves the right to award negotiated contracts to one or more Proposers. Proposals received shall be considered to remain in effect for no less than six (6) months and for no more than eighteen (18) months from the date of receipt.

IMPORTANT: APPLICATIONS THAT ARE NOT 100% COMPLETE AS SPECIFIED WITHIN THIS RFP, EXCEED THE SPECIFIED PAGE LIMITS, OR ARE NOT RECEIVED BY THE SPECIFIED DUE DATE AND TIME WILL NOT BE REVIEWED. ACCORDINGLY, PLEASE READ THE INSTRUCTIONS CAREFULLY SINCE CRITICAL INFORMATION IN THESE REGARDS MIGHT ONLY BE PRESENTED ONE TIME.

The BPHC will only contract with firms that do not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability, marital status, sexual orientation, citizenship status, or any other status protected by Commonwealth of Massachusetts and Federal laws.

All service contracts awarded by the Boston Public Health Commission may be subject to following the City of Boston's living wage ordinance. This ordinance requires that all employees working on sizable city contracts earn an hourly wage that is enough for a family of four to live at or above the federal poverty level. This wage amount called the living wage, is recalculated every year. For more information, please visit <https://www.boston.gov/worker-empowerment/living-wage-division>.

As part of BPHC's efforts to have an equitable procurement process, BPHC will consider and encourage Certified Unrepresentative Businesses Enterprises(CUBE) that includes; Minority-owned Business Enterprises (MBE), Women-owned Business Enterprises (WBE), Veteran-owned Business Enterprises (VBE),Disability-owned Business Enterprise (DOBE), Lesbian Gay Bisexual Transgender Business Enterprises (LGBTBE), Minority Non Profit(MNPO), Women Non Profit(WNPO), Minority Women Non Profit(MWNPO) and local businesses to apply to this RFP.

II. PROPOSAL SCHEDULE & APPLICATION REQUIREMENTS

07/25/2025	Advertisement on the Boston Globe
07/25/2025	Posted on boston.gov/bids by 10:00 AM EST
08/04/2025	Questions due via email to RFR@bphc.org by 5:00 PM EST: Subject – HIPAA Privacy & Security Assessment
08/13/2025	Responses to questions available for viewing boston.gov/bids by 5:00 PM EST
08/22/2025	Proposal due via email by 5:00 PM EST: Subject – HIPAA Privacy & Security Risk Assessment - ITS-001-26 Email: RFR@bphc.org NO EXCEPTIONS TO THIS DEADLINE
09/08/2025 – 09/09/2025	Vendor Interviews (if needed)
09/15/2025	Notification of Decision: Desired date to award. BPHC has the discretion to extend this time period without notice to the proposers. All proposals shall remain valid and open for a period of one hundred twenty (120) days from the proposal submission date, unless a proposer notifies BPHC of its withdrawal.
11/17/2025	HIPAA Privacy & Security Assessment to be completed

By November 17, 2025, the risk assessment must be finalized. At the end of this engagement, the service provider will have conducted a comprehensive Information Security Risk assessment of BPHC's policies, procedures, PHI, and Information Technology Assets. The first deliverable will be a Risk Assessment Report by November 6, 2025. The Roadmap should be delivered by November 17, 2025.

A. APPLICATION REQUIREMENTS

- This RFP is funded by the Center for Disease Control's Collaboration with Academia to Strengthen Public Health. The funding source Award Number is NE11OE000085 and it is active through 11/30/27. Any proposal must comply with BPHC Regulations, CDC Regulations and the Federal Uniform Guidance, eCFR 200
- Each proposal shall be prepared simply and economically, avoiding the use of elaborate promotional materials beyond what is sufficient to provide a complete, accurate and reliable presentation. An **eleven-point Font or larger, standard 8.5 inch by 11-inch paper, single-spaced with margins no smaller than 1 inch** are to be used for all materials (except for the Fonts, margins and paper size used on BPHC provided forms). **All documents are to include page numbers.**
- **PROPOSALS ARE TO BE SENT IN THE FOLLOWING MANNER:**
One **(1) digital copy** email to RFR@bphc.org.

BPHC RFP Submission Package Checklist (labeled as Appendix A).

1. **Application Cover Page** (labeled as **Appendix B**). The original must have an original signature of an authorized representative of the lead applicant organization.
2. **Vendor Profile**. The Vendor Profile is to be limited to **no more than four (4) pages**. **The Scoring Tool is included in this package (Appendix C) and should be reviewed in order to maximize your score.**
3. **Description of the proposed solution and work plan, including timeline and deliverables**. This requirement is limited to **no more than five (15) pages**. **The Scoring Tool is included in this package (Appendix C) and should be reviewed in order to maximize your score.**
4. **Responsible Bidder Attestation.**
5. **Disclosure of Employees or Officers of Boston Public Health Center**. A letter indicating the name, title and department of any employee or officer of Boston Public Health Commission within the 12 months immediately before the proposal. If none, indicate such in your letter.
6. **References**. A list of at least three (3) references from a Public Agencies organization with knowledge and experience with the specific services being offered.
7. **List of Prime Contractors and Subcontractors**. A list of prime contractors and subcontractors that the vendor does business with related to the services being offered in this RFP.
8. **Roles and Resumes of staff that will be assigned to this project.**
9. **Proposer Certification**. Include completed and signed Proposer Certification, with original signature, included as **Schedule A**.
10. **Response to Section B – Project and Long-Term Costs**. This should be submitted as a separate Section B.

B. HOW TO APPLY

To the extent feasible, please order your narrative content and the other proposal materials consistent with that indicated in **Section II B. Application Requirements**. If the ordering contradicts submission ordering directions in other sections of this RFP there will no penalty for any resultant document ordering discrepancies in your submission.

Submission of the proposals shall be directed to:

RFR@bphc.org

RFP# Information Security Risk Assessment Service – No: ITS-001-26

Boston Public Health Commission

All proposals must be delivered by August 22, 2025 BY 5:00 PM EST. Proposals received after the above date and time will not be considered. Absolutely no exceptions will be made. The Boston Public Health Commission is under no obligation to return proposals.

- NO COMMUNICATIONS OF ANY KIND WILL BE BINDING AGAINST THE BPHC, EXCEPT FOR THE INFORMATION TECHNOLOGY SERVICES FORMAL RESPONSES TO QUESTIONS, IF ANY, ADDRESSED ON THE WEBSITE.
- Proposers may be required to give an oral presentation to the BPHC to clarify or elaborate on their written proposal. Those Proposers will be notified to arrange specific times.
- No proposal will be accepted from, nor any agreement awarded to any Proposer that is in arrears upon any debt or in default of any obligation owed to the Boston Public Health Commission. Additionally, no agreement will be awarded to any Proposer that has failed to satisfactorily perform pursuant to any prior agreement with the Boston Public Health Commission.
- **Optional:** In case of a Certified Minority Business Enterprise/Women's Business Enterprise (MBE/WBE) vendor. The proposers must include the Commonwealth of Massachusetts Supplier Diversity Office (SDO) Certification letter with their proposal.
- **Optional:** In case the proposer is a Veteran-Owned Business, Proposer should include a letter indicating the company is 51% or more Veteran-owned.

Please note that BPHC will not review material beyond the specified page limits.

III. SCOPE OF PROFESSIONAL SERVICES REQUIRED

A. OBJECTIVE

The HIPAA Privacy & Security Risk Assessment should provide a comprehensive evaluation of HIPAA compliance and security risks including the ability to detect and mitigate cybersecurity threats. In addition, the assessment should provide Information security guidance that is fully aligned with industry standards and best practices and methodologies outlined in National Institute of Standards and Technology (NIST), Cyber Security Framework (CSF), Top 18 CIS Controls, HIPAA, and ISO/IEC, etc.

The evaluation should include a roadmap to be used to develop a plan for remediation of any identified items.

B. GOAL

The goal of the assessment is to identify and validate weaknesses in the BPHC's policies, procedures, information security architecture, physical controls and posture from both an internal and external vantage point.

C. SCOPE OF WORK

The following tasks outline the functional areas in which the Service provider shall assess in this engagement.

Penetration Testing

The scope of the Penetrating test is to identify exploitable security weaknesses in an information system and determine effectiveness of security controls. The test should include the entire perimeter and any critical systems that may impact the security of the systems. This includes both the external perimeter (public-facing attack surfaces) and the internal perimeter (LAN to LAN attack surfaces).

Perimeter Testing

The service provider shall test BPHC's network perimeter both externally and internally. In addition, the test must include critical systems that could affect the security including security systems (e.g. firewalls, authentication servers, etc.) or any assets utilized by privileged users to support and manage the systems.

Activities must include, but may not be limited to:

Perform an in-depth Information Security vulnerability assessment and penetration testing of BPHC IT infrastructure of:

- **External network** - all external public-facing systems including firewalls, FTP, web servers, and web service interface points.
 - Enumerate systems on the network and validate them against known systems. Identify any unknown or unexpected systems.

- Scan network systems and mainframe for potential vulnerabilities. BPHC will provide the network ranges and any network/host exemptions to these scans.
- Perform analysis of incoming and outgoing traffic security practices.
- Identify, analyze, and confirm vulnerabilities. It is expected that qualified service provider personnel will know how to look deeper into potential vulnerabilities for other security holes, misconfigurations, and other problems in order to follow the vulnerability to its end. It is expected that the service provider will share method and process (i.e., e-mail's screen shots, files, etc.) of successful penetration in addition to a list of open ports, missing patches, or possible vulnerabilities.
- The security vendor will conduct security risk assessment scans on 25 critical applications.
All vulnerabilities reported as Critical/High shall be detailed in the 'Findings' section of the final deliverable. A complete list of vulnerabilities shall be provided in a separate appendix. Each vulnerability or risk identified shall be categorized as a Critical/High, Medium, or Low.
The service provider shall attempt to capture user credentials through the collection of the following vectors:
 - Windows password hashes in-memory
 - Keystroke logging
 - Password and hash sniffing
 - Collecting saved login credentials
- **Internal network** – all internal systems including routers, switches, physical and virtual servers, data storage infrastructure, public computers and other connected IT devices: including all Demilitarized (DMZ) systems to include flow of controls from external and internal systems.

User Privilege Escalation

Throughout the assessment, the service provider shall attempt to complete user privilege escalations in order to further compromise, or demonstrate the effectiveness of, the security of established controls within BPHC's environment.

This test will assist in determining if access control systems are effectively enforcing user access and permission levels are configured correctly based on job function.

Segmentation Testing

The service provider shall test the segmentation controls of all segregated network segments from a sample of completely isolated/segmented networks (ensuring that each type of segmentation point is represented, such as firewalls, VLAN on switch, etc.).

Wireless Scanning (both private and guest)

The service provider shall identify rogue wireless devices and additional security architecture weaknesses related to the wireless networks.

Applications

Provide authenticated application vulnerability scanning and penetration testing (At a minimum, the test should include OWASP Top 10). The security vendor will conduct security risk assessment scans on approximately 10 external facing applications.

- Identify application security vulnerabilities.
- Perform active exploit through identified vulnerabilities in web/mobile apps, and assess weaknesses in (Application Programming Interface) APIs.
- Session Management- Secure submission and authentication.
- (Note: Exploit should stop at the point of proof of compromise but not causing any business interruption).

Database Assessment

We have approximately 60 databases. In the database assessment phase, the service provider shall take the following actions:

- Assess the databases to look for common vulnerabilities such as buffer overflows, default accounts, or default permissions on database objects such as tables, views, and stored procedures.
- Look for erroneous configurations that may lead to information leaks, theft of data, or even intrusion and denial of service attacks.
- Examine several key functional areas that may include but not be limited to:
 - Authentication and Authorization to Control Database Access
 - Identify vulnerabilities with existing remote access.
 - Password Complexity Verification
 - Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
 - Server Security
 - Database Connections
 - Table Access Control
 - Audit controls
 - Physical controls
 - Encryption Usage
 - Certificate Application

Brute Force Attack

The service provider shall conduct brute force attack to check for weak passwords. The objective of this test is to confirm whether passwords are meeting security best practices.

Social Engineering (Phone and E-mail)

During the Social Engineering phase of the assessment, the service provider shall attempt to impersonate and persuade BPHC/EMS employees via telephone and/or e-mail to disclose proprietary information. This information may allow the service provider to access sensitive information and/or exploit the integrity and/or availability of data. The sophisticated methods that may be utilized are, but not limited to, as follows:

- **Employee Impersonation** – Calling employees and attempt to convince them to release sensitive information (e.g. passwords of systems, unpublished e-mail addresses, names of other employees, names and virtual locations of systems).
- **Pretexting** – This method is the act of creating and using an invented scenario to persuade a targeted victim to release information or perform an action and is typically done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, Social Security Number, last bill amount or other specific company information to establish legitimacy in the mind of the target).

PHI Inventory

- Create a detailed inventory of all PHI (electronic and hard copy) within BPHC.
- Identify PHI flow through BPHC, including storage, use, access, and transmission points.

Physical Controls

- Conduct onsite visits to assess common security and privacy related practices within and between departments to include, but not be limited to, disposal, storage, and encryption practices, procedures, building structure.
- Access controls such as access restrictions, media handling, workstation placement and security. Onsite visits will be performed at BPHC's discretion
- Evaluate if building or space modifications are required to comply with HIPAA Privacy and Security modifications.

Evaluation of Privacy Policies and Procedures

- Review existing BPHC policies to ensure they align with HIPAA requirements including compliance with HIPAA Privacy and Security Roles.
- Identify all information systems and communication networks that store, maintain, or transmit ePHI and determine compliance with HIPAA Security and Privacy regulations or other state security and privacy statutes.
- Evaluate the potential risks associated with how departments and activities collect, use, manage, house, disclose and dispose of protected health information and propose safeguards to meet HIPAA security and privacy regulations, OCR guidelines, or best practices for security of sensitive information.
- Review BPHC employee training programs with regard to HIPAA compliance and proper handling of client PHI and identify areas for ongoing training and awareness initiatives focusing on HIPAA compliance.
- Review consent and authorization forms for compliance with HIPAA requirements.

- Review current HIPAA structure and assess through interviews, if additional departments meet the definition of either a covered entity or business associate as defined in the HIPAA Rules.

Review the contents of BPHC's standard Business Associate Agreement (BAA) to ensure it complies with current HIPAA standards.

Access Control, Data Integrity, and Incident Response Procedures

- Review BPHC's procedures for granting, modifying, and terminating access to client PHI.
- Evaluate the effectiveness of physical and technical safeguards to restrict unauthorized access to client PHI.
- Review BPHC incident response procedures in the case of a breach or unauthorized access to PHI.

D. Out of Scope

- Phishing email test.
- Denial of Service is outside the scope of the Penetration Test.
- The vendor is required to prevent any disruptions that would lead to system outages.

E. REQUIRED DELIVERABLES

- Kickoff Meeting and Project Plan for the HIPAA Privacy & Security Risk Assessment.
- **Executive summary:** The executive summary should include high level overview of the assessment including the following:
 - Overall assessment results.
 - Overall risk ranking and key areas of risk.
 - Current maturity level score card against NIST Cybersecurity Framework.
 - Strategic recommendations and key areas of focus for remediation.
- **Detailed report:** The detailed report should include detail of the assessment including the following:
 - Assessment methodology
 - Detailed assessment results in a sortable spreadsheet, risk ranking and actionable recommendations for all areas within the assessment scope.
 - Detailed score card of current maturity level for each NIST subcategory
 - PHI Inventory
 - Identify threats to PHI.
 - Penetration test results and recommendations
- **Road map:** This should include both tactical and strategic recommendations in a risk-based approach with consideration of business environment, technology, people and process.
 - **Tactical recommendations:** This should identify issues that are tactical in nature, simple to implement, and will have a positive impact to overall NIST alignment and HIPAA compliance. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.

- **Strategic Recommendations:** This should identify issues that are strategic in nature, complex to implement, and require management decisions to fund, but will have a significant impact on the overall architecture program. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.
- **Appropriate milestones** and key performance indicators to enhance BPHC's information security posture and address key risk findings.
- **Identification of privacy & security projects** based on individual or combined recommendations with detailed activities and action plans.
- **An assessment** of how the implementation of each project would remediate risk and position BPHC with respect to industry best practices.
- **Prioritized project plan:** The project plan is developed to support the road map. At a minimum, the project plan should include the following elements:
 - Project description
 - Priority
 - Risk rank
 - Supported road map item #
 - Recommended solution
 - Level of complexity to implement
 - Resource requirement
- **Presentation deliverable:** The service provider should prepare and deliver an executive-level presentation of the assessment.

It is important to note that once the Information Security vulnerability assessment testing is completed, the Service provider must remove all agents, backdoors, any software used for the risk assessment project, thus removing any trace of existence in the BPHC IT infrastructure.

A summary of BPHC's devices is listed in the table below

BPHC Device	Approximate Count
Workstations	979
Servers	93
Data Centers	3
VLANs	95
Routers	3
Switches	105
Firewalls	2
Wireless locations	20
Access Points	175
UPS – Battery backups	64

F. PROPOSAL REQUIREMENTS

For Proposers to be considered for an award, the terms, conditions, and instructions contained in this RFP and attachments must be met. Any proposal which does not meet these criteria may be considered non-responsive. Your proposal should include two sections (A and B) and should be submitted in separate envelopes. **To maximize your score, please refer to the Scoring Tool in Appendix C.**

Section A: Staffing and Qualifications

This section shall describe the approach and plans for accomplishing the work outlined in the Scope of Service section. Each proposal shall be prepared simply and economically, avoiding the use of elaborate promotional materials beyond what is sufficient to provide a complete, accurate, and reliable presentation.

1. RFP Coversheet
2. Vendor Profile (Maximum: Four Pages)
 - Background
 - Date Founded
 - Organizational Structure
 - () Sole Proprietorship
 - () Partnership
 - () Corporation
 - Ownership Status
 - () Independent
 - () Subsidiary (Include Name of Parent Organization)
 - Company History
 - Office Locations, Personnel, and Expertise
 - Products and Services Offered
 - What is the vendor's years of experience, background, and track record in conducting Information HIPAA Privacy & Security risk assessment?
 - Indicate relevant credentials and industry certifications.
Provide a description of your firm's experience in performing similar work.
 - Professional Conduct
 - Describe any situation where a client has terminated a contract with vendor "for cause" claiming breach of contract.
 - Service Delivery Model
 - Any services delivered by off-shore (outside North America). If so, please provide details.
 - Any deliverables scoped, developed, tested, or supported by off-shore (outside North America) resources? If so, please provide details.
3. Provide a Description of the proposed service and work plan, including timeline and deliverables. (Maximum: Five Pages)

4. Include sample invoices that demonstrate the level of detail and standard billing format used for client charges.
5. Demonstrate that the bidder is a “responsible bidder” by attesting that the bidder:
 - Complies with all laws prerequisite to doing business in the Commonwealth of Massachusetts.
 - Complies with U.S. Equal Opportunity Employer provisions.
6. If applicable, Certified Minority Business Enterprise/ Women’s Business Enterprise (MBE/WBE) proposers should include the Commonwealth of Massachusetts Supplier Diversity Office (SDO) Certification letter with their proposal.
7. If applicable, Proposers who operate a Veteran-Owned Business should include a letter indicating their company is 51% or more veteran-owned with their proposal.
8. The name, title, and department of any employee or officer who was an employee or officer of the Boston Public Health Commission within the 12 months immediately before the proposal. If none, indicate such in your letter.
9. A list of at least three references from an organization with knowledge and experience with the specific services being offered.
10. A list of all prime contractors and subcontractors that their agency does business with related to the service in this RFP.
11. Roles and resumes of staff that will be assigned to this project.
12. Include the signed Proposer Certification (Schedule A.) with the original signature.

Section B – Project Costs

This section shall provide the direct and indirect costs for accomplishing the work outlined in the Scope of Service section. Please include a description, justification, and calculation for all budget lines.

Project Costs

1. Personnel Costs:
 - a. Total and hourly salaries for all personnel on the project.
 - b. Fringe Benefit-cost.
2. Travel (if applicable)
3. Equipment (if applicable)
4. Contractual (if applicable)
5. Other (if applicable)
6. Software Licenses

IV. STATEMENT OF RIGHTS

UNDERSTANDINGS

Please take notice, by submission of a proposal in response to this request for proposals, the Proposer agrees to and understands:

- That any proposal, attachments, additional information, etc., submitted pursuant to this Request for Proposals constitute merely a suggestion to negotiate with the Boston Public Health Commission.
- Submission of a proposal, attachments, and additional information shall not entitle the Proposer to enter into an agreement with the Boston Public Health Commission for the required services.
- By submitting a proposal, the Proposer agrees and understands that the Boston Public Health Commission is not obligated to respond to the proposal, nor is it legally bound in any manner whatsoever by submission of same;
- That any and all counter-proposals, negotiations, or any communications received by a proposing entity, its officers, employees or agents from the Boston Public Health Commission, its officers, employees or agents, shall not be binding against the Boston Public Health Commission, its officials, officers, employees or agents unless and until a formal written agreement for the services sought by this RFP is duly executed by both.

In addition to the foregoing, by submitting a proposal, the Proposer also understands and agrees that the Boston Public Health Commission has the right, and may at its sole discretion exercise, the following rights, and options with respect to this Request for Proposals:

- To reject any or all proposals;
- To issue amendments to this RFP;
- To issue additional solicitations for proposals
- To waive any irregularities in proposals received after notification to Proposers affected;
- To select any proposal as the basis for negotiations of a contract, and to negotiate with one or more of the Proposers for amendments or other modifications to their proposals;
- To conduct investigations with respect to the qualifications of each Proposer;
- To exercise its discretion and apply its judgment with respect to any aspect of this RFP, the evaluation of proposals, and the negotiations and award of any contract;
- To enter into an agreement for only portions (or not to enter into an agreement for any) of the services contemplated by the proposals with one or more of the Proposers;
- To select the proposal that best satisfies the interests of the BPHC and not necessarily on the basis of price or any other single factor;
- To interview the Proposer(s);
- To request or obtain additional information the Boston Public Health Commission deems necessary to determine the ability of the Proposer;
- To modify dates;
- All proposals prepared in response to this RFP are at the sole expense of the Proposer, and with the express understanding that there will be no claim, whatsoever, for reimbursement from the Boston Public Health Commission for the expenses of preparation. The Boston Public Health Commission assumes no responsibility or liability of any kind for costs incurred in the preparation or submission of any proposal;
- The Boston Public Health Commission is not responsible for any internal or external delivery

delays which may cause any proposal to arrive beyond the stated deadline. To be considered, proposals MUST arrive at the place specified herein and be time-stamped prior to the deadline.

Proposal Costs

Each Proposer shall be solely responsible for all costs and expenses associated with the preparation and/or submission of its proposal, and BPHC shall have no responsibility or liability whatsoever for any such costs and expenses. Neither BPHC nor any of its directors, officers, employees or authorized agents shall be liable for any claims or damages resulting from the solicitation or collection of proposals.

BPHC assumes no responsibility or liability for costs incurred by respondents to the Request for Proposal, including any requests for additional information, interviews, or negotiations.

By submitting a proposal, Proposer expressly waives (i) any claim(s) for such costs and expenses, and (ii) any other related claims or damages.

Disposition of Proposals

All proposals submitted in response to this RFP become the property of BPHC once they are opened.

Other Considerations

BPHC reserves the right to request additional information as may be required and to further investigate proposer's qualifications to make this determination.

EVALUATION

The following criteria, not necessarily listed in order of importance, will be used to review the proposals. The Boston Public Health Commission reserves the right to weigh its evaluation criteria in any manner it deems appropriate:

- Proposer's demonstrated capability to provide the services;
- Evaluation of the professional qualifications, background and resume(s) of individuals involved in providing services;
- Proposer's experience to perform the proposed services;
- Proposer's financial ability to provide the services;
- Evaluation of the proposed cost/s. It should be noted that while cost is not the only consideration, it is an important one;
- A determination that the Proposer has submitted a complete and responsive proposal as required by this RFP;
- An evaluation of the Proposer's projected approach and plans to meet the requirements of this RFP;
- The Proposer's presentation at and the overall results of any interview conducted with the Proposer;
- Proposers MUST sign the Proposal Certification attached hereto as "Schedule A". Unsigned proposals will be rejected;
- If applicable, Certified Minority Owned Business Enterprises and Women-Owned Business Enterprises (MBE/WBE) by the Commonwealth of Massachusetts – Supplier Diversity Office (SDO);
- Proposers may be required to give an oral presentation to the Boston Public Health Commission to clarify or elaborate on the written proposal; and
- No proposal will be accepted from nor any agreement awarded to any Proposer that is in arrears upon any debt. Additionally, no agreement will be awarded to any Proposer that has failed to satisfactorily perform pursuant to any prior agreement with the Boston Public Health Commission.

CONTRACT

After the selection of the successful Proposer, a formal written contract will be prepared by the Boston Public Health Commission and will not be binding until signed by both parties and, approved by the Boston Public Health Commission - Office of the General Counsel.

INDEMNIFICATION AND INSURANCE

The Proposer accepts and agrees that language in substantially the following form will be included in the contract between the Proposer and the Boston Public Health Commission:

“In addition to, and not in limitation of the insurance requirements contained herein the Consultant agrees:

- (a) that except for the amount, if any, of damage contributed to, caused by or resulting from the negligence of the Boston Public Health Commission, the Consultant shall indemnify and hold harmless the Boston Public Health Commission, its officers, employees, and agents from and against any and all liability, damage, claims, demands, costs, judgments, fees, attorneys' fees or loss arising directly or indirectly out of the acts or omissions hereunder by the Consultant or third parties under the direction or control of the Consultant; and
- (b) to provide defense for and defend, at its sole expense, any and all claims, demands or causes of action directly or indirectly arising out of this Agreement and to bear all other costs and expenses related thereto

Upon execution of any contract between the Proposer and the Boston Public Health Commission, the Proposer will be required to provide proof of the insurance coverage described in “Schedule B.”

Insurance coverage in amount and form shall not be deemed acceptable until approved by the Boston Public Health Commission.”

INTELLECTUAL PROPERTY RIGHTS

The Proposer accepts and agrees that language in substantially the following form will be included in the contract between the Proposer and the Boston Public Health Commission:

All deliverables created under this Agreement are to be considered “works made for hire.”. If any of the deliverables do not qualify as “works made for hire,” the Consultant hereby assigns to the Boston Public Health Commission all right, title and interest (including ownership of copyright) in such deliverables and such assignment allows the BPHC to obtain in its name copyrights, registrations and similar protections which may be available. The Consultant agrees to assist the BOSTON PUBLIC HEALTH COMMISSION, if required, in perfecting these rights. The Consultant shall provide the BOSTON PUBLIC HEALTH COMMISSION with at least one copy of each deliverable.

The Consultant agrees to indemnify and hold harmless the BOSTON PUBLIC HEALTH COMMISSION for all damages, liabilities, losses, and expenses arising out of any claim that a deliverable infringes upon an intellectual property right of a third party. If such a claim is made, or appears likely to be made, the Consultant agrees to enable the BOSTON PUBLIC HEALTH COMMISSION’s continued use of the deliverable, or to modify or replace it. If the BOSTON PUBLIC HEALTH COMMISSION determines that none of these alternatives is reasonably available, the deliverable will be returned.

All records compiled by the Consultant in completing the work described in this Agreement, including but not limited to written reports, source codes, studies, drawings, blueprints, negatives of photographs, computer printouts, graphs, charts, plans, specifications, and all other similar recorded data, shall become and remain the property of the BOSTON PUBLIC HEALTH COMMISSION. The Consultant may retain copies of such records for its own use.

NON-COLLUSION

The Proposer, by signing the proposal, does hereby warrant and represent that any ensuing agreement has not been solicited, secured or prepared directly or indirectly, in a manner contrary to the laws of the Commonwealth of Massachusetts and the rules of Boston Public Health Commission, and that said laws have not been violated and shall not be violated as they relate to the procurement or the performance of the agreement by any conduct, including the paying or the giving of any fee, commission, compensation, gift, gratuity or consideration of any kind, directly or indirectly, to any BOSTON PUBLIC HEALTH COMMISSION employee, officer or official.

CONFLICT OF INTEREST

All Proposers must disclose with their proposals the name of any officer, director or agent who is also an employee of the Boston Public Health Commission. Further, all Proposers must disclose the name of any BPHC employee who owns, directly or indirectly, an interest of ten percent or more in the firm or any of its subsidiaries or affiliates.

There shall be no conflicts in existence during the term of any contract with the BOSTON PUBLIC HEALTH COMMISSION. The existence of a conflict shall be grounds for termination of a contract.

COMPLIANCE WITH LAWS

By submitting a proposal, the Proposer represents and warrants that it is familiar with all federal, state, and local laws and regulations and will conform to said laws and regulations. The preparation of proposals, selection of Proposers, and the award of contracts are subject to provisions of all Federal, State, and BOSTON PUBLIC HEALTH COMMISSION laws, rules and regulations.

CONTENTS OF PROPOSAL

The federal Freedom of Information Act and the Massachusetts Public Records Law, mandates public access to government records.

**APPENDIX A:
BPHC SUBMISSION PACKAGE CHECKLIST
RFP# ITS-001-26**

**HIPAA Privacy & Security Risk Assessment
Services**

Proposer Name: _____

Place a check in the first column to indicate that each item is contained in your application package.
Materials should be compiled in the following order.

	APPENDIX A: RFP Submission Package Checklist
	APPENDIX B: Cover Page
	Vendor Profile (Maximum Four (4) pages)
	Description of the proposed solution and work plan, including timeline and deliverables. (Maximum Five (5) Pages)
	Sample Invoices
	Responsible Bidder Attestation
	Commonwealth of Massachusetts - Supplier Diversity Office (SDO): MBE/WBE Certification Letter (if applicable)
	Veteran-Owned Business Letter (if applicable)
	Disclosure of Employees Boston Public Health Commission
	References
	List of Prime Contractors and Subcontractors
	Roles and Resumes of Staff assigned to this project
	Proposer Certification
	Section B: Project Costs

APPENDIX B

COVER PAGE INSTRUCTIONS

BOSTON PUBLIC HEALTH COMMISSION HIPAA Privacy & Security Risk Assessment Services RFP # ITS-001-26 Appendix B: <u>PROPOSER COVER PAGE FORM - APPLICANT INFORMATION</u> Instructions for completing Appendix B	
Organization Name	Please list the official name of your organization.
Mailing Address	Please list the official address of your organization for mailing purposes; include city and ZIP code information.
Primary RFP Contact	Please provide name, telephone number, FAX number, email address and, complete mailing address if different than the organizational mailing address above, for the primary contact for this proposal. Should you have a change in this information after submitting your application, please be sure to provide the updated information to RFR@bphc.org .
Alternate RFP Contact	Please provide name, telephone number, FAX number, email address and, complete mailing address if different than organization mailing address above, for an alternate contact for this proposal. Should you have a change in this information after submitting your application, please be sure to provide the updated information to RFR@bphc.org .
Leadership	Please list the name of your organization's Executive Director, President or Chief Executive Officer. If your organization has interim leadership, please list "Interim" in parentheses.

Chief Executive Officer Signature (as identified above)

Date

Printed Name and Title

APPENDIX B:
COVER PAGE

BOSTON PUBLIC HEALTH COMMISSION HIPAA Privacy & Security Risk Assessment RFP # ITS-001-26 APPENDIX B: <u>AGENCY COVER PAGE - APPLICANT INFORMATION</u> Please refer to the instructions within the RFP for completing Appendix B. (This is to be the top sheet for the entire application package.)	
Organization Name:	
Mailing Address:	
Primary RFP Contact:	
Alternate RFP Contact:	
Leadership:	

Chief Executive Officer Signature (as identified above)

Date

Printed Name and Title