Request for Proposal
Questions and Responses
08/13/2025

Request for Proposal: HIPAA Privacy & Security Assessment
Proposal Due Date: 08/22/2025

Q1: We would like some additional guidance on the Privacy Risk Assessment (PRA). A PRA can be a very detailed audit with a review of each line item, including statutes, policies, and offered evidence, which can be time-consuming. Most of our clients favor a less 'audit-like' Privacy and Breach assessment, still evaluating risk and creating risk management plans, but using a more 'easily accessible' set of Privacy and Breach questions arising from HIPAA. Would you like us to quote both options? Both options include a complete document review, form review, and assessment.

A:

- 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.

- 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.

- 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.

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

Q2: *Will the selected vendor be able to install a testing appliance on the network with access to all of the subnets that will be tested?*

A:

- BPHC will provide the network ranges and any network/host exemptions to these scans.
- Rules of engagement will be provided to tester after vendor selection.

Q3: *How many facilities should be included in the on-site walkthrough portion of the audit? If you could provide a list of locations, that would be helpful.*

A: Onsite visits will include 1 to 7 Boston locations. Onsite visits will be performed at BPHC's discretion.

Q4: *The Required Deliverables section states that a HIPAA Security Risk Assessment and a current maturity level for each NIST subcategory should be included in the proposal. Are you requesting a full HIPAA Security Risk Assessment and a full NIST Cybersecurity Framework 2.0 Assessment?*

A: ***See answer to question #1.***

Q5: *A Scoring Tool (Appendix C) was referenced in the RFP, but was not included in the package. Please send it to us for review.*

A: The scoring tool is excluded from the RFP. References to the scoring tool will be removed.

Q6: *Are there any pre-approved time windows for penetration testing to avoid business disruption?* After 5pm

Q7: *Will BPHC provide explicit network ranges/host exemptions upfront, or will the vendor need to discover them?*

A: See answer to question #2.

Q8: *For external systems (firewalls, web servers), are there any restrictions on scanning intensity (e.g., rate limiting)?*

A:

- 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.
- (Note: Exploit should stop at the point of proof of compromise but not causing any business interruption).
- See answer to question #2

Q9: *For internal systems, will the vendor have access to all VLANs (95 listed), or only a subset?*

A:

- Up to 95
- 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.

Q10: *Beyond the listed devices (e.g., 93 servers, 105 switches), are there any legacy systems or IoT devices that require special handling?*

A: See the answer to question #2.

Q11: *For the 10 external-facing applications, will BPHC provide credentials for authenticated scans, or will the vendor test only unauthenticated surfaces?* Applications for authenticated scans will be provided after vendor selection.

Q12: *Are there specific OWASP Top 10 priorities (e.g., injection flaws, broken authentication) to focus on?*

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).

Q13: For the 60 databases, are they all relational (e.g., SQL Server, Oracle), or do they include NoSQL? Relational and MySQL

Q14: Will the vendor have read-only access to test configurations, or is a simulated attack required? **See answer to question 12.**

Q15: What employee groups (e.g., IT, HR, clinical staff) should be targeted for phone/email testing? Plan to target these groups. Phishing emails are out of scope.

Q16: Are there pre-approved scenarios (e.g., impersonating IT support), or can the vendor propose methods? Vendor can propose methods.

Q17: Should the inventory include third-party systems (e.g., cloud storage, EHR platforms) where PHI might reside? **Yes**

Q18: Is there a preferred format/tool (e.g., spreadsheet, GRC platform) for documenting PHI flows? Vendor should suggest the GRC platform for documenting PHI flows.

Q19: How many physical locations require onsite visits, and are there secure areas (e.g., data centers) with access restrictions? **Yes.. there are total of 10-12 physical locations.**

Q20: Should vulnerabilities be mapped to specific HIPAA Security Rule citations (e.g., §164.308(a)(1))?

- 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.
- **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.

Q21: Is there a preferred risk scoring framework (e.g., CVSS, DREAD)? **No**

Q22: Should recommendations align with NIST CSF tiers (e.g., Tier 3 "Repeatable") or another maturity model?

- 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.

Q23: Are tactical fixes (e.g., patch management) expected to be prioritized over strategic projects (e.g., architecture redesign)?

- **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

Q24: Are there restricted tools (e.g., Metasploit, Burp Suite) or preferred commercial tools (e.g., Nessus, Qualys)? No

Q25: Will BPHC provide SIEM/log data to correlate findings, or is the vendor expected to rely on scans alone? The vendor is expected to use their own tools.

Q26: Will the vendor be given privileged accounts for privilege escalation testing, or must they exploit weaknesses to gain access? No

Q27: Is there an expectation for post-remediation validation (e.g., rescanning critical systems after fixes)? This RFP does not cover the remediaton process.

Q28: Are there current security policies (e.g., password complexity, encryption standards) the vendor must validate against?

- 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.

Q29: Beyond HIPAA, should the assessment consider state-specific laws (e.g., MA 201 CMR 17.00) or HITRUST?

- 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.

Q30: If a breach is simulated (e.g., via successful exploitation), should the vendor document BPHC's response process?

- 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).

Q31: Are there blackout periods (e.g., fiscal year-end, audits) when testing must be paused? ***See answers above.***

Q32: Who are the key contacts for IT (e.g., network team), compliance, and executive reporting?
Presentation deliverable: The service provider should prepare and deliver an executive-level presentation of the assessment.

Q33: Should all findings/data be stored in BPHC's environment, or can the vendor use their:
Vendor can store findings in their own environment.

Q34: Are there knowledge transfer expectations (e.g., training sessions for BPHC staff on findings)? Refer to RFP document and required the deliverables section.

Q35: Can any work be performed by offshore teams, or must all personnel be North America-based?
A:

- 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.

Q36: Is BPHC open to exploring non-USA/offshore based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity professionals in a cost-efficient manner.
A: Refer to RFP and question answered in this document.

Q37: Can BPHC provide any information on the budget required to support these services? (E.g., budget details)

A:
Budget information is not provided in this RFP.

Q38: Is BPHC currently using any service providers that are assisting BPHC in performing the requested services? If so, who are these providers?
A: Refer to RFP for services to be performed.

Q39: How many employees are in scope for this RFP?
A: There are approximately 1400 BPHC employees.

Q40: How many policies are in scope?
A: Approximately 10 policies

Q41: We did not receive Appendix C or Schedule A. Could those be provided?
A: Appendix C Scoring Tool is excluded from RFP. Availability of Proposer Certification form to be determined. Proceed without it for now.

Q42: Does BPHC host all of your IT infrastructure? If not, what technology providers are involved? Will be provided to selected vendor. Do you have agreements with them that allow penetration testing?
A: Some are hosted by BPHC. ROE will be addressed with the vendor.

Q43: Are there any time restrictions when testing can be performed?
A: After 5pm

Q44: Can we export firewall rules so they can be consumed by tools for analysis?
A: Yes

Q45: Are the 25 critical applications in-scope all web applications? If not, what is the architecture and underlying platforms?
A: Mostly SaaS. SQL and Microsoft platforms.

Q46: Do you have an existing asset inventory that be leveraged for identifying systems with PHI?
A: Yes

Q47: Are BPHC offices shared with any other departments or entities?
A: Yes

Q48: RFP references reviewing alignment with HIPAA privacy and security requirements. Is the breach notification rule in-scope as well?
A: Refer to RFP and answered questions.

Q49: How many policies/procedures are in scope?
A: Refer to answered questions

Q50: How many buildings are included in the physical control scope?

A: See answered questions

Q51: *Are portions of the penetration testing, segmentation testing, and database assessments expected to be conducted onsite or is remote access sufficient?*
A: This is up to the vendor.

Q52*: For the physical control piece, are there any additional physical penetration testing techniques that are wanted, such as an Offensive Security walkthrough of the buildings on-site?*
A:

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.

Q53*: Will BPHC provide existing diagrams or inventories to aid in PHI flow and ePHI system mapping, or is full discovery required?* Yes
A:

Q54*: Can you share a copy of "Schedule B" outlining insurance requirements?*
A: Not available.

Q55*: On page 13, it states that " Your proposal should include two sections (A and B) and should be submitted in separate envelopes" but earlier mentions that our response must be submitted via email by August 22nd, at 5pm. Please clarify which way we should submit.*
A:
Proposal due via email by 5:00 PM EST. Email: RFR@bphc.org

Q56*: Is a sampling approach for testing the 60 databases acceptable?*
A:
Yes

Q57*: Two documents seem to be missing from the RFP: Appendix C (scoring tool) and Schedule 1 (Proposer Certification). Could the BPHC please supply these?*
A: Scoring Tool will not be published in this RFP. Availability of Proposer Certification form to be determined. Proceed without it for now.

Q58*: How many external IP addresses are in scope?*
A:
Refer to the RFP

Q59: *On page 8, the RFP mentions security risk assessment scans of 25 public-facing applications. On page 9, the RFP requests authenticated testing of 10 public-facing web applications. Please*

confirm that we are performing detailed (application-layer) testing of only 10 public-facing web applications.
A: The security vendor will conduct security risk assessment scans on approximately 10 external facing applications.

***Q60**: Are detailed firewall configuration reviews in scope? If so, are the two firewalls paired, or identically configured?*
A:

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.

Additional details to be addressed after vendor selection.

***Q61**: Are the wireless networks controller-based?*
A: There are controller based wireless networks.

***Q62**: How many locations are in scope for wireless network testing?*
A: Refer to the RFP Device table.

***Q63**: How many users should we target with social engineering?*
A: 200

***Q64**: Please confirm that social engineering tests should be phone-based only and that email-based exercises are out of scope.*
A: Phishing email test is out of scope.

***Q65**: Does BPHC have an existing inventory of all assets and systems that contain, store, process, or transmit ePHI?*
A: Refer to answered questions and RFP.

***Q66**: How many locations are in scope for the physical security controls assessment?*
A: See answered questions.

***Q67**: See to BPHC have a full set of formal, documented HIPAA security policies in place?*

A: BPHC has HIPAA and security policies.

***Q68**: Does BPHC have a full set of formal, documented HIPAA privacy policies, procedures, and forms in place? Are these documents enterprise-wide or customized by department?*

A: See answered questions.

***Q69**: How many unique departments or divisions within BPHC handle PHI?*

A: See answered questions.

***Q70 :** Approximately how many staff should we expect to interview to conduct the HIPAA assessment?*

A: To be determined after vendor selection.

***Q71**: Would you be able to quantify the **externally exposed infrastructure** across all relevant verticals—including but not limited to public IP addresses, internet-facing web applications, APIs, and any other externally accessible assets that should be included within the scope of the penetration test?*

A: Yes

***Q72**: Could you provide details regarding the **internal attack surface**, such as the number of internal hosts, applications, services, and network segments, so we can accurately define the internal testing scope?*

A: Refer to RFP.

***Q73**: For **web applications**, should we assume authenticated testing is required for all 10 applications? Will **test credentials** be provided?*

A: Refer to answered questions.

***Q74**: What kind of remote access (VPN, RDP, any other third-party access, etc.) possibilities would be provided by The Boston Public Health Commission for internal network assessment?*

A: Will address after vendor selection.

Q75: Could BPHC please confirm whether this is a new initiative or an existing engagement?

A: Refer to RFP

Q76: Could BPHC provide an estimated budget or a Not-to-Exceed (NTE) amount for this contract?

A: See answered questions.

Q77: Could BPHC please provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?

A: Refer to RFP.

Q78: Could BPHC please clarify whether it intends to award this RFP to a single vendor or multiple vendors? If multiple awards are anticipated, could BPHC specify the expected number of vendors to be selected?

A: Single vendor

Q79: What is the estimated budget range allocated for this engagement to help ensure our proposed scope aligns with BPHC's expectations?

A: See answered questions.

Q80: What is the expected project timeline, including the preferred start date and target completion deadline for all deliverables?

A: Refer to RFP

Q81: Is this engagement intended to be a one-time assessment, or does BPHC anticipate recurring services? If recurring, which components (e.g., penetration testing, vulnerability scanning, social engineering, policy reviews) should be included in the ongoing scope?

A: Refer to RFP

***Q82**: Will the penetration test be performed against production systems, or is a test/staging environment available?*

A: Production

***Q83**: How many external IP addresses and internal systems are expected to be included in the testing scope?*

A: Refer to the RFP

***Q84**: Are cloud-hosted systems or SaaS platforms included in the external perimeter test?*

A: Refer to RFP.

***Q85**: Will BPHC provide whitelisting, credentials, or VPN access for testing restricted areas?*

A:
See answered questions.

***Q86**: Is the penetration testing limited to discovery and exploitation (proof-of-concept), or does it require full exploitation chain reporting?*

A: See answered questions. Refer to RFP.

***Q87**: Are there any legal or compliance constraints (e.g., testing hours, critical systems exclusions) that must be followed during the engagement?*

A: Yes

***Q88**: Are there legacy systems or unsupported platforms that require specialized testing techniques?*

A: See answered questions

***Q89**: Is lateral movement expected to be simulated in internal testing?*

A: Refer to RFP, including the Perimeter Testing section and Deliverables.

***Q90**: Will the penetration test be performed against production systems, or is a test/staging environment available?*

A: See answered questions.

***Q91**: How many external IP addresses and internal systems are expected to be included in the testing scope?*

A: Will address after vendor selection.

***Q92**: Are cloud-hosted systems or SaaS platforms included in the external perimeter test?*

A: Refer to RFP.

***Q93**: Will BPHC provide whitelisting, credentials, or VPN access for testing restricted areas?*

A: Yes

***Q94**: Is the penetration testing limited to discovery and exploitation (proof-of-concept), or does it require full exploitation chain reporting?*

A:
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. Refer to RFP for more information.

***Q95**: Are there any legal or compliance constraints (e.g., testing hours, critical systems exclusions) that must be followed during the engagement?*

A: ROE will be addressed after vendor selection.

Q96: Are there legacy systems or unsupported platforms that require specialized testing techniques?

A:
Refer to the RFP

Q97: Is lateral movement expected to be simulated in internal testing?

A:

Q98: What is the total number of IPs, domains, and endpoints expected to be tested externally?

A:

See answered questions. Refer to RFP.

Q99: Will you provide a complete network architecture diagram or list of segmented zones for internal testing?

A: See answered questions.

Q100: Are virtual systems (VMs, containers) part of the internal infrastructure to be tested?

A: refer to scope of work in RFP.

Q101: What controls (e.g., NAC, IDS/IPS) are currently in place at the perimeter that we need to test against?

A: Will discuss whitelisting.

Q102: Are vendor-managed appliances or third-party systems part of the perimeter environment?

A: Yes

Q103: What is the policy for scanning devices connected via VPN or remote desktop?

A: Rules of engagement, restrictions and additional information will be provided by BPHC after vendor selection.

Q104: How often is BPHC currently conducting vulnerability assessments?

A: Refer to RFP for scope of work.

Q105: Should this assessment include configuration reviews of servers and workstations?

A: See answered questions. Refer to RFP.

Q106: Are internal and external vulnerability scans expected to be run multiple times, or just once?

A: See answered questions. Refer to RFP.

Q107: Should vulnerability validation (false positive removal) be included in the scope?

A: See Scope of Work, and deliverables. Refer to RFP.

Q108: Will access be provided to credentialed scanning for OS- and patch-level visibility?

A: See answered questions.

Q109: Are there systems (e.g., medical equipment, legacy hardware) that must be excluded from active scanning?

A: See answered questions.

Q110: Should both horizontal and vertical privilege escalation attempts be simulated?

A: Refer to RFP.

Q111: Are privilege escalation tests expected on workstations, servers, and Active Directory?

A: Refer to RFP

Q112: Will access be provided to test accounts with varying privilege levels?

A: See answered questions

Q113: Is the environment domain-joined or decentralized (e.g., multiple domains or identity stores)?

A: Will address after vendor selection.

Q114: Are you expecting a red team-style simulation or a more controlled test plan?

A: Refer to RFP.

Q115: Should we attempt to pivot across segments after escalation?

A: Refer to RFP.

Q116: How many VLANs or segmented networks are in scope for segmentation testing (from the 95 listed)?

A:
Segmentation Testing

The service providers hall 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.). Refer to RFP for more information.

Q117: Will access be granted to validate inter-VLAN communication, or must bypass attempts be simulated?

A: See answered questions and refer to RFP.

Q118: What segmentation controls (e.g., firewalls, ACLs, VLAN tags) are in place and should be tested?

A: See answered questions and refer to RFP.

Q119: Are there critical systems that must not be disrupted even in non-invasive segmentation tests?

A: See answered questions and refer to RFP.

Q120: Will testing be done from representative systems or directly from vendor equipment?

A: See answered questions.

Q121: Do you expect east-west traffic flow testing within each segment?

A: Refer to RFP.

Q122: Will the vendor have physical access to all 20 wireless locations for on-site scanning?

A: Yes

Q123: Are separate guest and corporate wireless SSIDs in place, and are both in scope?

A: Refer to RFP.

Q124: Should rogue device detection cover both access points and connected clients?

A: Plan to cover access points and connected clients.

***Q125**: Is wireless password strength analysis and protocol security configuration testing expected?*

A: Refer to RFP.

***Q126**: Should signal leakage testing (i.e., coverage beyond intended physical areas) be performed?*

A: Yes

***Q127**: Is Bluetooth testing or BLE beacon scanning also part of this engagement?*

A: Will address after vendor selection.

***Q128**: What are the technology stacks (e.g., Java, .NET, PHP, Node) of the 10 external applications?*

A: Will address after vendor selection.

***Q129**: Will you provide full credentials for authenticated scanning of all application roles?*

A:

See answered questions.

***Q130**: Are mobile apps included in the scope, and if so, for which platforms (iOS/Android)?*

A: Refer to RFP.

***Q131**: Should testing include session management, CSRF, and access control logic?*

A: Refer to RFP.

***Q132:** Are APIs publicly documented, or should testing teams reverse-engineer them?*

A: Will address after vendor selection.

***Q133**: Are third-party libraries and dependencies part of the scope for Software Composition Analysis (SCA)?*

A: Will address after vendor selection.

***Q134**: What database technologies are included among the ~60 databases (e.g., MS SQL, Oracle, MySQL)?*

A: See answered questions.

***Q135**: Will test credentials and documentation (e.g., ERDs, schemas) be provided for each database?*

A: See answered questions.

***Q136**: Is this assessment intended to include performance-impacting testing, or just safe configuration auditing?*

A: Refer to RFP.

***Q137**: Will privileged access be granted to assess user permissions and stored procedures?*

A: See answered questions.

***Q138**: Is encryption-at-rest/in-transit in use, and should it be verified per instance?*

A:

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.

***Q139**: Are backup databases and logs part of the review scope?*

A: Refer to RFP

***Q140**: Is brute-force testing expected on external login portals or internal systems only?*

A: See answered questions. Refer to RFP.

***Q141**: Are there time/attempt limits or monitoring mechanisms that may block accounts during testing?*

A: Yes, will discuss whitelisting

***Q142**: What authentication methods are in use (e.g., MFA, LDAP, SAML, local)?*

A: Will address after vendor selection.

***Q143:** Will test accounts be provided for brute force attempts?*

A: Refer to answered questions.

***Q144**: Are dictionary/wordlist-based attacks acceptable, or should only targeted logic-based testing be used?*

A: This will be addressed after vendor selection.

***Q145:** Are CAPTCHA or lockout thresholds implemented, and should they be tested?*

A: Refer to RFP.

***Q146**: How many users or departments should be targeted for phone and email-based social engineering?* Phishing emails are out of scope.

A: Refer to answered questions.

Q147: *Should deep reconnaissance (e.g., OSINT profiling) be part of the approach?*

A: Refer to RFP. Details will be discussed after vendor selections,

Q148*: Are there pretexting scenarios preferred (e.g., IT support, HR, vendor impersonation)?*

A: No

Q149*: Is live call recording permitted for documentation of results?*

A: Plan for live calls.

Q150*: Are any departments (e.g., Legal, Security) off-limits for social engineering testing?*

A: See answered questions.

Q151*: Are email-based payloads (e.g., phishing documents) allowed if they don't deliver malware?*

A: See answered questions. Refer to RFP

Q152: *Is social engineering expected to be a one-time engagement or a recurring activity (e.g., weekly, monthly simulations or campaigns)?*

A: See answered questions and refer to RFP.

Q153*: Does BPHC already maintain a PHI asset inventory that can be reviewed or updated?*

A: See answered questions.

Q154*: Are vendors expected to conduct interviews with business process owners to discover PHI flows?* Plan to conduct interviews with business owners.

A:

***Q155**: Is digital and hard copy PHI in equal scope?*

A: Will address after vendor selection.

***Q156**: Are backup tapes, offsite records, or physical storage cabinets in scope?*

A:

***Q157**: Are departments required to provide data flow diagrams or should vendors create them?*

A: See answered questions. Refer to RFP.

***Q158**: What PHI classification levels (sensitive, restricted) does BPHC use?*

A: Refer to RFP.

***Q159**: How many physical locations are expected to be assessed?*

A: See answered questions.

***Q160**: Will vendors be escorted, or will they have full independent access during onsite visits?*

A: Will address after vendor selection.

***Q161**: Should physical media handling (e.g., paper shredding, USB use) be tested?*

A: Refer to RFP.

***Q162**: Are CCTV, badge systems, and alarm controls expected to be reviewed?*

A: Refer to RFP. Will address additional questions after vendor selection.

***Q163**: Are vendors expected to attempt physical intrusion or tailgating tests?*

A: Physical intrusion or tailgating tests are not included in RFP.

***Q164**: Is the review focused on HIPAA-aligned physical control safeguards only, or broader facility security?*

A: Refer to RFP

***Q165**: How many HIPAA-related policies and procedures are expected to be reviewed?*

A: See answered questions. More information will be addressed after vendor selection.

***Q166**: Are policies centralized, or does each department maintain its documentation?*

A: Mostly centralized

***Q167:** Will past audit findings or OCR corrective actions be shared for context?*

A: See answered question

***Q168:** How many departments are currently identified as covered entities or business associates?*

A:

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

***Q169**: Will employee training records be shared, or must vendors conduct assessments via interview?*

A: Will address after vendor selection.

Q170: Are policies expected to be mapped to specific HIPAA rules (e.g., 164.308, 164.312)?

A: Refer to RFP.

Q171: Will access control logs be made available for review (e.g., IAM systems, AD audit trails)?

A: Will be discussed after vendor selection.

Q172: Is access provisioning/deprovisioning centralized or handled by each department?

A: Will be discussed after vendor selection.

Q173: Are there identity federation or SSO platforms in place (e.g., Okta, Azure AD)?

A: Will be discussed after vendor selection.

Q174: Will vendors review previous incident reports or perform simulations?

A: Will be discussed after vendor selection.

Q175: How is PHI access currently monitored or audited (e.g., DLP, SIEM)?

A: Will be discussed after vendor selection.

Q176: What incident response playbooks or policies currently exist, if any?

A: Will be discussed after vendor selection.

External Testing

Q177: Are any third-party hosted applications or services (e.g., hosted websites, SaaS apps) included external testing? Yes

Should scans be non-authenticated, or will credentials be provided for authenticated scanning? See answered questions.

Is there an existing vulnerability management platform in place (e.g., Tenable, Qualys)? If so, will access be provided? Vendor should plan to use their own tools.

Internal Testing

How will internal access be provided? (e.g., VPN, virtual machine, physical access)

Are any systems off-limits for testing (e.g., SCADA, medical equipment, legacy systems)? See answered questions.

Is the internal network primarily Windows, Linux, or a mix of both? See answered questions.

Will domain credentials be provided for auditing Active Directory? See answered questions.

How many Active Directory domains or forests exist, and are they all in scope? 2

Is the environment dependent on cloud/third party systems/services such as Azure, AWS, etc.? If so will these be included in scope? Yes, plan to test third party systems.

Will scanning agents be permitted for internal assets? See answered questions.

Segmentation Testing

How many unique network perspectives will be required for segmentation testing? See answered questions.

Can you identify critical segmentation points (e.g., firewall, VLAN trunk)? 95 VLANs.

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.). Refer to RFP for more details.

Are there any air-gapped or segmented networks? If so, how many? Yes. Will address after vendor selection.

Wireless

What is the approximate travel time between each of the 20 wireless locations? 30-40 min approx travel time.

Will access be granted for non-guest wireless networks? Will address after vendor selection.

Are there any known wireless devices we should exclude? Refer to RFP.

In addition to scanning, will the test team be allowed to deploy rogue access points? Will address after vendor selection.

Will deauthentication attacks be allowed against wireless clients? Refer to RFP and answers above regarding disruption of service

Applications

Are the applications commercial off-the-shelf (COTS), custom-built, or a mix of both? Will discuss after vendor selection.

Will both privileged and non-privileged accounts be provided for testing? See answered questions.

Are there APIs in use? Will API documentation (e.g., Swagger/OpenAPI) be provided? See answered questions and refer to RFP.

Are any third-party hosted applications (SaaS) in-scope? See answered questions.

Database Assessment

Please provide a list of database types, versions, and approximate quantity per type.

Will direct database access be provided (e.g., credentials, SQL clients, connection strings)?

See answered questions.

Can we test stored procedures and role-based access control? Plan to include procedures and role-based access control.

Social Engineering

How many separate Social Engineering tests are desired? Refer to RFP.

Will a list of target personnel be provided? See answered questions.

Will targets/context require prior approval? See RFP. Will discuss in more detail after vendor selection.

How many employees will be targeted during phone/email-based social engineering? See answered questions.

Are there specific departments (e.g., IT, HR, finance) we should focus on? See answered question

Will the targets be aware of the test (i.e., authorized deception)? Refer to RFP.

Are there specific pretexts you want or don't want us to use? See answered questions.

Can we spoof internal phone numbers or email domains? Will discuss after vendor selection.

Section D. lists "Phishing email test" as out of scope, can you clarify if Social Engineering is limited to phone/in-person testing, or if phishing emails are also included? Phishing emails are out of scope.

PHI Inventory

Will you provide a list of systems that store or process PHI? See answered questions.

Do you have existing data flow diagrams that outline PHI usage? See answered questions.

How is PHI currently protected (e.g., encryption, physical access control)?

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.

Refer to RFP for more information

Physical Controls

Approximately how many physical locations will be tested? See answered questions.

Will we have access to all physical locations, or are there any off-limits areas? Refer to RFP

Are there any specific physical controls we should be aware of (e.g., mantraps, biometric access)? Will discuss after vendor selection.

Are physical badge access systems or surveillance systems in scope? See answered questions. Will address additional questions after vendor selection.

Should we include tailgating, piggybacking, or other physical access tests such as lock picking/bypassing? See answered questions.

Will we be escorted during physical testing, or will this be a covert engagement?

See answered questions.

Evaluation of Privacy Policies and Procedures and Access Control, Data Integrity, and Incident Response Procedures

How many pages of policy documents are included to review? See answered questions.

How much training material (unit metric pages, slides, or video time) are included in review? Refer to RFP.

Does privacy considerations include the draft of proposed Massachusetts Data Privacy Act? Refer to RFP.

Questions: Application Testing Scope

Can BPHC provide a full list of the ~25 applications included in the assessment scope? Will discuss after vendor selection. See answered questions.

Please clarify: Are these standalone applications, modules within an EHR/PM system, or third-party cloud/SaaS tools? Yes

For the five (5) critical applications mentioned, what are the application types and technologies involved? Will discuss after vendor selection. See answered questions.

Web-based, client/server, mobile, cloud-hosted (e.g., AWS, Azure), etc.? See answered questions. Refer to RFP.

What type of access will be provided for application testing? See answered questions.

Will BPHC provide test credentials, sandbox environments, or production access with limitations?

See answered questions.

What specific types of application testing are required?

- 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).

Is the expectation limited to authenticated and unauthenticated web application vulnerability scanning (e.g., OWASP Top 10)? See answered questions. Refer to RFP.

Or does BPHC require full dynamic testing (DAST), static testing (SAST), and/or business logc testing? See answered questions and refer to RFP.

Are APIs or integrations with external services part of the scope? See answered questions.

If yes, how many APIs or integration points are expected to be evaluated?

- Perform active exploit through identified vulnerabilities in web/mobile apps, and assess weaknesses in (Application Programming Interface) APIs. Refer to RFP for more information.

Questions: HIPAA, PII, and Policy/Procedure Audits

Will BPHC provide existing HIPAA Privacy & Security policies, training logs, or documentation for review? Yes

What specific artifacts should we plan to review (e.g., security policies, breach notification plan, encryption standards)? Refer to RFP

What internal teams or roles will be available for interview during the audit phase? Yes

(e.g., privacy officer, IT security, HR, clinical operations) Yes

What PII-related systems or data flows outside of the main EMR/EHR applications should be included in the assessment? Will address after vendor selection.

e.g., HR systems, billing, transportation, mental health or substance abuse program systems?

See answered questions.

Is the expectation that the selected vendor will assess policy implementation in addition to documentation?

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.

Will the audit involve walkthroughs or control testing for physical safeguards, access controls, and incident response? See answered questions. Refer to RFP.

Has BPHC undergone a previous HIPAA risk assessment or OCR audit? Yes

If yes, can the findings or reports be shared to inform this engagement? Previous assessment findings are not included in this RFP.