UNIONCOUNTY
north carolina

Request for Proposals 2023-026

HIPAA Risk Assessment

ADDENDUM No. 2

ISSUE DATE: February 7, 2023

Responding Offerors on this project are hereby notified that this Addendum shall be made a part of the above named RFP document.

The following items add to, modify, and/or clarify the RFP documents and shall have the full force and effect of the original Documents. This Addendum shall be acknowledged by the Offeror in the RFP document.

Add/Delete/Replace

A. <u>Delete/Replace</u>

1. **Delete in its entirety:** In Section 4, Project Scope, last two sentences in paragraph, page 6:
   ~~Subsequent action plan should be laid out to address gaps in compliance and security. Parallel to this process should be an expert legal analysis and determination of all programs and applicability to requirements under HIPAA.~~
   <u>Replace with:</u> Subsequent action plan should be laid out to address gaps in compliance and security and should include expert guidance that assures compliance with HIPAA guidelines. Each submitting vendor should provide information demonstrating that your company has expertise in the area of compliance with HIPAA regulations and guidelines.

2. **Delete in its entirety:** ~~Appendix A – Price Form~~
   <u>Replace with:</u> Appendix A – Addendum #1 Price Form (***Refer to page 22 of this addendum)***

B. <u>Question/Answer Section</u>

1. **Question:** The RFP requests that the legal analysis to determine applicability to HIPAA occur "in parallel". That may mean assessment work occurs on departments that are identified as non-applicable during the legal analysis. Have you considered doing the legal analysis in advance?

   Answer: In response to this question, please refer to section A. Delete/Replace item #1

2. **Question:** Do you an incumbent?

   Answer: No

3. **Question:** Will the assessment for the departments all start at the beginning of the assessment or are they spread out at different times?

   Answer: Yes

4. **Question:** The parallel legal review mentioned in the RFP, will this be the responsibility of the company awarded the HIPAA contract?

   Answer: In response to this question, please refer to section A. Delete/Replace item #1

5. **Question:** Have you considered leveraging the legal services to secure client-attorney privilege?

   Answer: In response to this question, please refer to section A. Delete/Replace item #1

6. **Question:** When reviewing the county Human Services ‘s Privacy Policies, is the selected vendor expected to consider preemption analysis of Privacy Rule to any State laws addressing privacy of health information?

   Answer: If you feel that adds value to your proposal if not cost prohibitive it is acceptable to include but not a mandate.

7. **Question:** The RFP Section 4.2 lists the Privacy Rule Standards to be assessed as **§**164.502(b) and **§**164.530 (a) through (i). Is the selected vendor expected to assess the County Human Services Department's compliance with all Standards of the Privacy Rule **§** 164.500- **§**164.530?

   Answer: What is referenced in the Security Rule should cover the risk assessment

8. **Question:** Would the HIPAA Risk Assessment include the three "TBD" systems identified in Section 4.3, or just include the seven electronic record systems currently listed?

   Answer: They will be completed by the time of the initial assessment.

9. **Question:** Section 4.1 Deliverables
   Legal research and recommendations on the delineation between covered and noncovered departments within Human Services and the application of HIPAA law for our consolidated agency both to meet compliance and to assure best practice in areas that are not covered.
   Is the expectation to have the opinion of the auditor backed by legal interpretation or seek the recommendation from legal counsel?

   Answer: The intention is for the auditor to provide expert guidance that assures compliance with HIPAA guidelines.

10. **Question:** Section 4.3 Areas of Assessment in Union County Human Services
    Under the 7 electronic record systems, 3 are listed as TBD. Do those systems share interdependency with any of the other systems in scope? Would excluding impact the evaluation of controls that may be inherited from another system in scope?

    Answer: No

11. **Question:** Are any of the record systems developed in-house or hosted by third party service providers?

    Answer: Hosted by third party

12. **Question:** Are all departments under the umbrella of the IT Department for support or is there departments that might have their own IT support functions?

    Answer: Union County has a central IT department that supports the County. Union County Human Services and Union County Jail have onsite IT support that operates under the oversite of the Central IT department.

13. **Question:** Do all departments adhere to one common set of policy and procedures, or do they maintain their own set of policies and operating procedures?

    Answer: Each department has their own set of policies and operating procedures.

14. **Question:** Section 4.4 Outcomes
    - Evaluation of clinical practices (e.g., interaction with patients, handling of PHI and ePHI) and compare those practices against written policies and procedures to include but not limited to virtual components.

- What is the expectation in evaluating interaction with patients? Is this by observation or an examination of written protocols?

Answer: Both. Expectation is to review policies and procedures for compliance and audit compliance with policies by observing relevant clinical practices.

15. **Question:** Will you provide scoping information for the pen test?

    Answer: Yes

16. **Question:** Will you complete a scoping document for us? At a minimum, number of internal/external IPs, count of subnets, level of segregation. Is it to be scoped to just the departments in the RFP?

    Answer: Yes, document can be provided at the onset of the project

17. **Question:** The RFP mentions that you'll need a second and final penetration test. Did a previous vendor perform an initial penetration test? Would we need to perform two, the second being remediation testing of the findings from the initial assessment?

    Answer: Perform two, the second being remediation testing of the findings from the initial assessment.

18. **Question:** For the penetration test and ePHI scanning, can you provide an estimated number of endpoints that will be in scope? Is your infrastructure located on-premises or hybrid-cloud?

    Answer: On premises. Up to 256 addresses associated with 6 subnets.

19. **Question:** Regarding the penetration test:
    1. How many external IPs are in scope?
    2. How many internal IPs are in scope?

    - How many external IPs are in scope?

    Answer:2

    - How many internal IPs are in scope?

    Answer: Up to 256 addresses associated with 6 subnets.

20. **Question:** Related to RFP section 4.1
    1. Do you want penetration testing performed and/or vulnerability scanning? We can do either or both, however we typically do vulnerability scanning to identify risks associated to specific systems. Vulnerability scans typically cover more systems and are not as costly as penetration testing. HIPAA regulations do not specify either, but we agree one or both of these should be included.
    2. Have vulnerability scans or penetration tests been performed on Union County Human Services within the last 12 months?
    3. See Appendix A: Questions by Service

- Do you want penetration testing performed and/or vulnerability scanning? We can do either or both, however we typically do vulnerability scanning to identify risks associated to specific systems. Vulnerability scans typically cover more systems and are not as costly as penetration testing. HIPAA regulations do not specify either, but we agree one or both of these should be included.

Answer: We would like the option to do both.

- Have vulnerability scans or penetration tests been performed on Union County Human Services within the last 12 months?

Answer: Not specifically on HHS, there has been one completed across the County in the last 12 months

- See Appendix A: Questions by Service

Answer: Not applicable

21. **Question:** Does Union County intend to provide a data map of ePHI within the areas of assessment and potentially an interdepartmental flow of ePHI between the areas of assessment in section 4.3?

    Answer: No

22. **Question:** What other documentation does Union County intend to provide to facilitate the determination of how and where PHI and ePHI is collected?

    Answer: None

23. **Question:** Are all of the in-scope departments subject to HIPAA or is that part of what we are helping Union County determine?

    Answer: No, we know some are not but would like guidance in determining applicability (covered entity vs. hybrid classification).

24. **Question:** Are all clinics electronically billing for health services?

    Answer: Yes

25. **Question:** During the Pre-Proposal Conference you indicated that each area uses the same information technology department. Are there any exceptions to this or does each agency use the same IT organization but with different applications?

    Answer: No

26. **Question:** How many physical locations are in scope?

    Answer: 4

27. **Question:** Related to RFP sections 4.3 & 4.4
    1. Are all locations and devices in scope accessible from one location?
    2. See Appendix A: Questions by Service

- Are all locations and devices in scope accessible from one location?

Answer: Yes (however the expectation is that this is not a fully remote assessment)

- See Appendix A: Questions by Service

Answer: Not applicable

28. **Question:** Is the County self-insured for healthcare claims, and do they pay health care claims individually?

    Answer: Yes, and yes.

29. **Question:** For Veteran's Services, is the County contractually obligated under any federal contracts to provide these services?

    Answer: No

30. **Question:** Will each of the areas of assessment (departments) have their own dedicated risk assessment reporting?

    Answer: Our goal is to assure continuity in compliance across departments so having one reporting would be preferable with the ability to isolate findings to department and program if needed.

31. **Question:** For the evaluation of technology design architecture, did you need us to perform a firewall/network design review or an Office 365 configuration review?

    Answer: No

32. **Question:** For the evaluation of physical security controls, how many and what types of locations would be in scope?

    Answer: 4 physical locations to include Health and Human Services, Transportation Services, and Veteran's Services, and Union County Jail.

33. **Question:** For the evaluation of telecommunications, will you need social engineering conducted via vishing assessment? Will you need any other form of social engineering testing performed?

    Answer: No

34. **Question:** For the consideration of applications, local/wide area network integrity and disaster recovery, will you need any tabletop incident response testing performed or ransomware simulation?

    Answer: No

35. **Question:** Is there any additional information for each department that we can access to assist in pricing? (number of employees per division/department, IT functions all centralized, etc.)

    Answer: Approximately 482 staff in HHS

36. **Question:** What is the timeframe anticipated between the first and second penetration test?

    Answer: 3-6 months

37. **Question:** How many reports will be required for the penetration testing? One report with an update/appendix to findings after an agreed-upon timeframe, or two separate reports?

    Answer: 2

38. **Question:** Will verbal review of documented pentest raw findings and formal findings be required?

    Answer: No

39. **Question:** Is this an assessment or an audit? Language such as “management response” is typically an audit, particularly given the RFP language to fulfill “admissible report for Federal and State audits” and a “qualified” opinion.

    Answer: We are seeking a risk assessment that also provides guidance on the actions necessary to be compliant with HIPAA standards.

40. **Question:** Are all Assessment Standards (14) applicable to all service areas (20) and all Record Systems (7) + (3) TBD? Only a portion are specifically called out in the RFP.

    Answer: The standards specified in the RFP should be sufficient.

41. **Question:** Does “legal research” related to having an attorney in the process (provided by the vendor) or conducting the risk assessment against the legislation of HIPAA requirements?

    Answer: Conducting the risk assessment against the legislation of HIPAA requirements.

42. **Question:** Is the Risk Management Plan related to just gaps found in the assessment? Or does the County desire to “effectively management risk” for all risks going forward?

    Answer: We are seeking to identify gaps though the risk assessment and expert guidance on how to effectively manage any gaps in accordance with HIPAA standards.

43. **Question:** For the Clinical Area – Will we need to see patient data to verify practices are handled as documented?

    Answer: No

44. **Question:** Will on-site visits be required to see how clinical practices are being handled in waiting room or checkout areas?

    Answer: Yes

45. **Question:** Similarly, for physical controls, are interviews sufficient or does testing include physical testing/observation?

Answer: Should include physical assessment and observation of practices.

46. **Question:** Will breach information be evaluated, i.e., evidence of response to previous breach notifications?

    Answer: No

47. **Question:** Is it fair that report sections should contain those services that do have PHI and those that do not?

    Answer: Yes

48. **Question:** Does the assessment include review of controls with BAA? Or just verification that BAA is in place where needed?

    Answer: Verification that BAA is in place

49. **Question:** Can we please receive clarity around “evaluation of the necessity of BAA related to vendors?” Does this mean vendors should have a BAA but do not?

    Answer: We are seeking assurance that having a BAA in place makes sense for all Human Services functions.

50. **Question:** How many HIPAA privacy and security officers exist?

    Answer: One HIPAA privacy officer located in Human Services department and one security officer located in County IT department.

51. **Question:** How many endpoints?

    Answer: Approximately 450

52. **Question:** Is bring your own device (BYOD) allowed?

    Answer: No

53. **Question:** Of the 400+ users, how many are full time employees versus contractors?

    Answer: There are approximately 12 contract staff

54. **Question:** Is remote access to EHR allowed?

    Answer: Yes

55. **Question:** Are the seven electronics record systems all in the cloud? All on-premise? Hybrid?

    Answer: Currently all on premise

56. **Question:** How many policies, procedures, and practice documents related to information technology and information security exist today?

    Answer: Approximately 7

57. **Question:** How many employee's take HIPAA Training?

    Answer: All staff in DSS, Health, Business Operations, Community Support and Outreach.

58. **Question:** Is the HIPAA training done annually?

    Answer: Yes

59. **Question:** What platform is the HIPAA training done on?

    Answer: Combination of in person training and virtual self-paced

60. **Question:** Is there a HIPAA Subject matter expert in the organization?

    Answer: There is a designated HIPAA privacy officer

61. **Question:** Has the organization experienced a breach of Protected Health Information?
    1. If so, was the breach reported to the Office of Civil Rights timely?
    2. If so, how many people were affected and what type of information was affected? i.e; social security numbers, Date of Birth, diagnosis, addresses, etc.

    - Has the organization experienced a breach of Protected Health Information?

    Answer: Not that we are aware

62. **Question:** Are there policies related to HIPAA and Protected Health Information?
    1. Are the policies on a public facing site?

    2. How many policies exist?

    - Are there policies related to HIPAA and Protected Health Information?

    Answer: Yes

    - Are the policies on a public facing site?

    Answer: No

    - How many policies exist?

    Answer: Approximately 25

63. **Question:** How many HIPAA violations on average happen within the organization on an annual basis?

Answer: None that we are aware

64. **Question:** Is there disciplinary action that occurs when there are violations?

    Answer: Yes, per internal policies

65. **Question:** Does the organization want the entire engagement to be performed under attorney-client privilege?

    Answer: In response to this question, please see the revision made to the RFP

66. **Question:** The RFP states that the contract award will have an initial term of 2 years. Does this mean that this entire engagement will occur once in 2023 and again in 2024 at the same cost each year?

    Answer: The expectation is that there is an annual risk assessment but the extent necessary in subsequent years could vary.

67. **Question:** Can we provide a cost per building for the physical security review instead of dividing it by department? If so, can you please provide the listing of buildings, addresses, and the departments within?

    Answer: Yes

68. **Question:** Can we provide a single cost for the penetration test if all of the networks are connected?

    Answer: Yes

69. **Question:** Can we provide a single cost for the HIPAA Risk Assessment for each collective of departments that share the same policies? If so, can you please provide the listing of departments that share the same policies?

    Answer: In general departments don't share policies.

70. **Question:** When was the last HIPAA Risk Analysis performed?

    Answer: Self-assessment was performed last in 2022. Last contracted risk assessment occurred in 2019.

71. **Question:** When was the last internal/external penetration test performed?

    Answer: May 2021 County wide

72. **Question:** Roughly how many individuals are on staff?

    Answer: Approximately 482

73. **Question:** Roughly how many servers and workstations are in the organization?

    Answer: 13 servers, roughly 450 workstations

74. **Question:** When does your organization want the active portions of the penetration test conducted?

    Answer: During business hours

75. **Question:** How many total IP addresses are being tested?
    1. How many internal IP addresses (estimated), if applicable?
    2. How many external IP addresses (estimated), if applicable?
    3. Please provide the number of IP addresses per department (if cost must be divided by department).

    - How many internal IP addresses (estimated), if applicable?

    Answer: 6 subnets, up to 256 addresses

    - How many external IP addresses (estimated), if applicable?

    Answer: 2 up to 64 subnets, not all in use

    - Please provide the number of IP addresses per department (if cost must be divided by department).

    Answer: Up to 256 each

76. **Question:** Wireless
    1. How many wireless networks are in place?
    2. Can wireless names be provided upon contract award?
    3. Approximately how many clients will be using the wireless network?

    - How many wireless networks are in place?-

    Answer:33

    - Can wireless names be provided upon contract award?

    Answer: Yes

    - Approximately how many clients will be using the wireless network?

    Answer: unknown

77. **Question:** Can the organization provide email addresses for a phishing test?

    Answer: Yes

78. **Question:** Physical security test -
    1. What are the addresses of the building(s) or office suite(s) to be assessed?
    2. What is the approximate square footage of the target(s)?

3. What is the use of the target location(s)? Office, manufacturing, storage, etc.
4. Are these properties owned or leased? If leased, who is the leasing company?

- What are the addresses of the building(s) or office suite(s) to be assessed?

Answer:

i. Union County Human Services: 2330 Concord Ave., Monroe, NC 28110
ii. Union County Transportation: 1407 Airport Rd., Monroe, NC 28110 (will be at this location by time of assessment)
iii. Union County Jail: 3344 Presson Rd., Monroe, NC 28112
iv. Union County Veterans Services: 407 N. Main St., Monroe, NC 28112

- What is the approximate square footage of the target(s)?

Answer:

i. Union County Human Services: 143,728 sq. ft.
ii. Union County Transportation: 1,430 sq. ft. (of office space. Will be in this space by time of assessment)
iii. Union County Jail: 23,000 sq. ft. (office space)
iv. Union County Veterans Services: 3,428 sq. ft.

- What is the use of the target location(s)? Office, manufacturing, storage, etc.

Answer: Office/Jail

- Are these properties owned or leased? If leased, who is the leasing company?

Answer: Owned

79. **Question:** In Appendix A, the County separates out the HIPAA Assessment Service and various costs thereunder from the Legal Service. The Legal Service is limited to "One-time Legal Research and Recommendations per section 4.1 of RFP," which refers solely to "legal research and recommendations on the delineation between covered and non-covered departments within Human Services and the application of HIPAA law for our consolidated agency both to meet compliance and to assure best practice in areas that are not covered."
    1. Has the County previously designated HIPAA covered and non-covered components among its departments, or is it seeking to have a hybrid entity evaluation and proposed designation performed for the first time?

    2. Does the language in Appendix A regarding Legal Service and the language in section 4.1 of the RFP indicate that the County does not desire legal review or input regarding compliance with HIPAA, including (for example) (a) whether the policies, procedures and practices between covered and non-covered components of the County are appropriate, (b) evaluation of the appropriate policies and practices to protect PHI the County uses to provide logistics and support to vaccine clinics, and (c) confirmation that the County's Business Associate Agreements contain sufficient language and are being used appropriately with applicable third parties? In other words, is the County looking for non-attorney advice and assessment of its compliance with HIPAA except as stated in section 4.1?

- Has the County previously designated HIPAA covered and non-covered components among its departments, or is it seeking to have a hybrid entity evaluation and proposed designation performed for the first time?

Answer: The County has previously designated HIPAA covered and non-covered components and is seeking expert guidance on the application of polices that are consistent across divisions that are both non-covered and covered entities.

- Does the language in Appendix A regarding Legal Service and the language in section 4.1 of the RFP indicate that the County does not desire legal review or input regarding compliance with HIPAA, including (for example) (a) whether the policies, procedures and practices between covered and non-covered components of the County are appropriate, (b) evaluation of the appropriate policies and practices to protect PHI the County uses to provide logistics and support to vaccine clinics, and (c) confirmation that the County's Business Associate Agreements contain sufficient language and are being used appropriately with applicable third parties? In other words, is the County looking for non-attorney advice and assessment of its compliance with HIPAA except as stated in section 4.1?

Answer: Yes, the County is looking for non-attorney advice and assessment of its compliance with HIPAA. Please also see revision to Section 4.1, above.

80. **Question:** Should time, travel, and materials be highlighted in the proposal or should that information be divided among the different sections of the price form?

    Answer:. All price information should be included in the price form.

81. **Question:** What is the function of the *Binding Authority?* Is this related to liability insurance?

    Answer: The binding authority is dealing with the authorize company/ corporate officer that has authority to sign contract agreement.

82. **Question:** Can the point of contact and the person with *Binding Authority* be the same?

    Answer: Yes

83. **Question:** Has Union County previously been sanctioned for HIPAA violations? If so, have those violations been remediated?

    Answer: Not that we are aware

84. **Question:** Will the previous HIPAA Risk Assessment be made available to the award winner?

    Answer: Yes

85. **Question:** How many servers are in the environment?

    Answer: 13

86. **Question:** How many external and internal IP addresses make up the network?

    Answer:
    1. 2 external IPs up to 64 addresses (not all in use)
    2. 6 internal IPs up to 256 addresses

87. **Question:** How many total endpoints are in the organization?

    Answer: 450

88. **Question:** How many remote users are in the organization?

    Answer: Approximately 50 but it varies

89. **Question:** Is there a Bring Your Own Device (BYOD) policy in the organization?

    Answer: No

90. **Question:** Is there an inventory list of all vendors that deal with PHI available?

    Answer: That can be provided.

91. **Question:** Three electronic record systems were listed as TBD (To be determined). When will those be defined?
    1. Transportation Electronic Management System
    2. Veteran's Services Software
    3. Behavioral Health Collaborative Software

    - Transportation Electronic Management System

    Answer: Most likely will be defined by onset of the project

    - Veteran's Services Software

    Answer: Will be defined by onset of the project

    - Behavioral Health Collaborative Software

    Answer: Will be defined by onset of the project

92. **Question:** How much time is available for all services to be completed once the award is granted?

    Answer: Services should be completed by the end of the calendar year to satisfy annual assessment requirements

93. **Question:** What security tools have been implemented to protect PHI currently?

    Answer: Multi Factor Authentication implemented in 2022 and best practices have been implemented to protect PHI

94. **Question:** Is there a requirement for all resources to be based in the United States if these resources are full time employees of our firm?

    Answer: Yes

95. **Question:** Will remediation be a consideration after the assessment is complete?

    Answer: No

96. **Question:** Should our quote be based on the annual cost of services or should we assess the two-year term cost?

    Answer: We would like both options

97. **Question:** Is there a possibility for the assessment scope to change after the award has been granted?

    Answer: Possibly

98. **Question:** How long after the submission will a decision be made to select a proposal OR to interview?

    Answer: Not available at this time.

99. **Question:** Has this function been contracted out before and if so, can you provide any information regarding the group currently performing the work (i.e. number of staff, company name, etc)?

    Answer: Not available at this time.

100. **Question:** Is there a limit as to how many people Union County is expecting to fill the role/s for this solicitation?

    Answer: Not available at this time.

101. **Question:** Are there particular licenses/certifications that Union County is expecting? CISSP, CHPSE, PMP, etc… The RFP notes a request to note licenses but are there specific ones that Union County requires?
    Answer: No

102. **Question:** In order to properly prepare our solicitation, can you please provide the respective sizes of each sector to be assessed on Page 7/8?
    1. Estimated # of people (400 + is noted near the end but next major bullet point identifies the question we have)
    2. Estimated # of physical facilities to be assessed
    3. Estimated # of computers
    4. Estimated # servers
    5. Estimated # printers
    6. Estimated # scanners- approximately

7. Estimated # of IoT / Mobile devices (IoT, internet of things (items like web cams, temperature sensors, remote monitoring of network enabled medical devices (EEGs, EKGs, Nurses Station monitors, etc…)))

- Estimated # of people (400 + is noted near the end but next major bullet point identifies the question we have)

  Answer: Approximately 480

- Estimated # of physical facilities to be assessed

  Answer: 4

- Estimated # of computers

  Answer: approximately 450

- Estimated # servers

  Answer:13

- Estimated # printers

  Answer: approximately 77

- Estimated # scanners

  Answer: approximately 93

- Estimated # of IoT / Mobile devices (IoT, internet of things (items like web cams, temperature sensors, remote monitoring of network enabled medical devices (EEGs, EKGs, Nurses Station monitors, etc…)))

  Answer: Not available at this time

103. **Question:** The RFP on page 8 notes 400 + users, is that 400 + users in total or just 400 + users at Business Operations?

Answer: In total

104. **Question:** Do we have to register to be considered for this request? The RFP does not note a registration requirement but there is an application to enter on the eVendor Portal System.

Answer: No

105. Question: Page 6, Section 4.1 Deliverables:
How is the County defining an "admissible report"?

Answer: A report that meets HIPAA expectations.

106. **Question:** Are two pen tests envisioned, one early in the assessment and a second to validate that control gaps have indeed been closed?

Answer: Yes

107. **Question:** An "improvement plan" is mentioned; can you confirm that this plan is to be part of our report, but ultimately executed by the County in the future?

Answer: Yes

108. Question: Page 6, Section 4.1 Deliverables:
The scope includes a time period for the County to make system corrections, what is the anticipated review period and scope of the secondary assessment limited to corrective actions taken?

Answer: Time period between the assessment and secondary assessment should be 3-6 months to allow a reasonable time for the County to make corrections but within the year to satisfy HIPAA requirements.

109. **Question:** What is the scope of the penetration test? (e.g. what type of technology, how many IP addresses, will it need to be authenticated, etc.)

Answer: A penetration test scoping document can be provided at the onset of the project.

110. **Question:** Has the organization undergone an exercise to determine which HIPAA controls are addressable?

Answer: No

111. **Question:** "Risk management plan that provides steps to effectively manage risk", which risk management framework does the county currently utilize?

Answer: We currently do not have a named framework but work collaboratively with our cyber security insurance provider to mitigate risk

112. Question: Page 7, Section 4.3 Areas of Assessment in Union County Human Services:
How many physical facilities are in scope for review of physical security controls?

Answer: 4

113. Question: Page 8, Section 4.3 Areas of Assessment in Union County Human Services:
For pen testing, can the County provide a size of its IT environment by answering these questions:

Answer:

Question	Count	Type
How many Desktops / laptops	450	(approx.) desktops/laptops/tablets

How many Servers	13	
How many Databases	10	
Routers and Switches	9	
Publicly Available IP addresses	2	
Number of internally reachable IPs	6	
Physical locations	4	Office Building, Jail
# of remote employees	50	varies
# Wireless Access Points	33	

114. **Question:** Several Electronic Health Records (HER) systems are mentioned; does the scope include conducting Meaningful Use assessments of those CEHRs?

Answer: No

115. Question: Pages 9-10, Section 4.4 Outcomes:

Does the first bullet imply that the vendor needs to do a data discovery to identify the presence and behavior of PHI and ePHI?

Answer: Yes

116. **Question:** The HIPAA evaluation requires modeling costs of failure in an associated exploit results in a breach; is this an "order of magnitude" model or something more granular?

Answer: Order of magnitude

117. **Question:** The 7th bullet describes a security architecture design evaluation; how complete and detailed does the County see this evaluation?

Answer: A detailed evaluation is not needed.

118. **Question:** How many departments are in scope for evaluation of their business continuity and IT disaster recovery plans? Does the county want an evaluation and improvement recommendation of these, or to re-write them to best practices?

Answer: Improvement recommendations

119. **Question:** How is the County using the term "Functional Needs Registry", can you elaborate?

Answer: The Union County Functional Needs Registry gathers key information (including PHI i.e. physical or mental impairments) from participants and can be referenced by Emergency Workers in the event of a disaster such as a hurricane, flood, winter storm, power outage, disease outbreak or nuclear event, etc.

120. Question: Pages 9-10, Section 4.4 Outcomes:
"Assessment of Human Services' HIPAA policies, procedures, and controls presently in place, and the effectiveness of those policies, procedures, and controls." Is the county interested in an audit of operating effectiveness of these controls?

Answer: Yes

121. Question: Page 11, Section 5.2 Proposal Format:
Can the County please confirm if title page, cover letter, tabs and staff resumes to be included in a response are NOT included in the 25 page limitation of the proposal response.

Answer: Yes

122. Question: Page 13, Section 5.2.3 Section 3 Staff Experience:
Can the County please clarify if staff resumes are required as part of a response to this Section?

Answer: Yes

123. **Question:** If resumes are required is there a page limitation for resumes?

Answer: No limitation

124. **Question:** If resumes are required will they be exempt from the 25 page limitation of the proposal response?

Answer: No

125. Question: Page 17, Section 5.6 Conflict Certification:
The text for this section reads "The Offeror must certify that it does not have any actual or potential conflicts of interest with, or adversarial litigation against the County or any of its officers or employees."

1. Can the County please clarify if this statement of certification of no conflicts (actual or potential) should be included in an appendix to the proposal response and, if so, will be exempt from the 25 page limitation of the proposal response?

Answer: Add to an appendix, no it will not be part of the 25 page count.

126. Question: Page 17, Section 6.1 Terms and Conditions:
Does the County anticipate that the work will take 2-3 years, or does this elongated contract period and extension imply that the County expects the vendor to contact a second HIPAA SRA over that 2-3 year time period?

Answer: The County expects annual HIPAA Risk Assessments

127. Question: Page 18, Section 6.4 Exception to the Proposal:
The text for this section reads "All exceptions taken must be identified and explained in writing in the proposal and must specifically reference the relevant section(s) of this Proposal."

1. Can the County please clarify if any exceptions noted should be included in an appendix to the proposal response and, if so, will be exempt from the 25 page limitation of the proposal response?

Answer: Yes, you can state your exemptions. The 25 page limitation is not exempt.

128. Questions:
Are resources required to be physically on site in Union County?

Answer: To the extent needed for evaluation of physical controls

129. **Question:** Do all resources need to be located in continental US?

Answer: Yes

130. **Question:** Do all persons have to be US Citizens?

Answer: No

131. **Question:** What applications are considered in-scope across departments?

Answer: The electronic record systems noted in the RFP.

132. **Question:** Do all in-scope departments have common policies, procedures, and technology infrastructure?

Answer: Common technology infrastructure but separate policies and procedures generally.

133. **Question:** Is IT centralized across all County departments?

Answer: There is a centralized County IT department and dedicated Jail and Human Services IT staff that operate under the general guidance of County IT.

134. **Question:** Does the scope include the HIPAA Privacy Rule?

Answer: Yes

135. **Question:** What is the anticipated timeline to start?

Answer: As soon as contract is finalized.

136. **Question:** How many assessments are anticipated over the 2 year contract period?

Answer: We require annual assessments.

137. **Question:** Has any informal internal HIPAA risk assessment been undertaken by the County in the last five years?

Answer: Yes

138. **Question:** Has the County suffered any HIPAA privacy or security breaches in the last five years that have resulted in an investigation or enforcement action by the HHS Office of Civil Rights?

Answer: Not that we are aware

139. **Question:** Has the County suffered any privacy or security breach that has resulted in reporting to a State oversight entity in the last five years?

Answer: Not that we are aware

140. **Question:** Does the County and/or any of the agencies mentioned in the RFP have a Chief Privacy Officer and/or Chief Security Officer?

Answer: The County has an Information Systems Coordinator designated as the HIPAA Privacy Officer and has an Information Systems Security Officer

141. **Question:** The RFP mentions that one deliverable is a report that would be admissible for Federal and State audits. Is an analysis of NC State privacy or security laws part of the scope of the RFP?

Answer: No

142. **Question:** The RFP mentions a review of Business Associate Agreements but not a general review of vendor agreements with County vendors that have access to PHI. Is this more general review part of the scope of the RFP?

Answer: No

143. **Question:** Can the county disclose its budget parameters for this scope of work?

Answer: No

ATTACHMENT: APPENDIX A – ADDENDUM #1 PRICE FORM

End of Addendum No. 2

1 APPENDIX A – ADDENDUM #1 PRICE FORM

RFP 2023-026 HIPAA Risk Assessment

Submit with Proposal

Company Name _____

Please provide the assessment cost for each Department as outlined in section 4.3 of the RFP document and in the following chart. The County reserves the right to increase or decrease Department services as deemed necessary.

A)

	HIPAA Assessment Service	**Cost**
1	**Division of Public Health**	
1.a	Public Health Clinic	$
1.b	Dental Clinic	$
1.c	Inmate Health Program	$
2	**Division of Social Services (DSS)**	
2.a	Eligibility Programs	$
2.b	Child and Adult Services Programs	$
2.c	School Collaborative Program	$
2.d	Child Support Enforcement	$
3	**Community Support & Outreach**	
3.a	WIC Program	$
3.b	Eligibility Programs	$
3.c	Senior Nutrition	$
4	**Transportation Services**	
4.a	Registration	$
4.b	Scheduling	$
5	**Veteran's Services**	$
6	**Business Operations**	
6.a	Information Technology Department	$
6.b	Records and Information Security Department	$
6.c	Public Health Billing and Registration Department	$
6.d	Public Health Preparedness Program	$
6.e	Customer Service Department	$
6.f	Language Services	$
Total		$

B)

	Legal Service	**Cost**
1	One-time Expert Recommendations for HIPAA Compliance per section 4.1 of RFP	$

A+B= Total Cost_____