Emergence Health Network
El Paso Center for Mental Health/Intellectual Disabilities

201 E. Main St., Suite 600
El Paso, TX 79901
(915) 887-3410
Fax: (915) 774-0201

ADDENDUM

To: All Interested Proposers

From: Erin Silva, Purchasing Manager

Date: July 17, 2020

Subject: Request for Proposal RFP #20-002 “HIPAA Security Risk Analysis”
Addendum I

This addendum includes:
Correction to the “Scope” section located on Pg. 4. of the RFP, under 45 CFR 163.306 General Requirements
Responses to all questions submitted as of Friday July 14, 2020

Reminder: RFP due August 7, 2020

Except as otherwise stated below and by any previous and subsequent Addenda, the above referenced Request for Proposal (RFP), remains unchanged. Furthermore, this Addendum is hereby made part of the contract documents.

Any questions or additional information required by interested vendors must be emailed to bidquestions@ehnelpaso.org . RFQ number and title must be on the “Subject Line” of the email. Attempts to circumvent these requirements may result in rejection of the proposal.

Emergence Health Network
El Paso Center for Mental Health/Intellectual Disabilities

HIPAA Security Risk Analysis
RFP No. 20-002
Response to questions raised by potential proposers (7/14/2020)

Correction to the Scope located on page four (4) of the RFP.

164.308 Administrative Safeguards
164.310 Physical Safeguards
164.312 Technical Safeguards
164.316 Policies; Procedures and Documentation
164.502 Uses and Disclosures of Protected Health Information-General Rules
164.504 Uses and disclosures: Organizational requirements.
164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
164.508 Uses and disclosures for which an authorization is required.
164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.
164.514 Other requirements relating to uses and disclosures of protected health information.
164.520 Notice of privacy practices for protected health information.
164.522 Rights to request privacy protection for protected health information.
164.524 Access of individuals to protected health information.
164.526 Amendment of protected health information.
164.528 Accounting of disclosures of protected health information.
164.530 Administrative requirements.

Responses to all questions submitted as of Friday July 14, 2020

Q. How many departments handle PHI/ePHI?

A. 80% of the departments at the center handle PHI/ePHI

Q. How many clinical departments need evaluation?

A. All of them

Q. How many non-clinical practices are in clinical facilities?

A. 0

Q. How many cloud providers would be in-scope?

A. 2

Q. How many applications are to be considered in-scope?

A. 2

Q. Do you have a documented disaster recovery plan?

A. In progress

Q. Can all testing take place from one location?

A. Penetration testing and interviews can be done remotely and 3 site visits at different locations.

Q. Page 5, Bullet 15. You ask for a second, final penetration test but we did not see an initial requirement for a penetration test. Is there to also be a penetration test? If so, for the entire environment?

A. We require an initial pen test; two weeks for finding remediation; and a second pen test for reporting purposes.

Q. Page 31, Pricing Sheet. Are we to propose recurring assessments for 3 years?

A. Yes, one test per year for 3 years.

Q. Are you also seeking on-going support pricing?

A. Yes

Q. What is the budget for this project?

A. Not dependent on budget

Q. If we submit a copy of our proposal via email are we expected to also send a hard copy to the corporate address?

A. No

Q. Page 8, Financial Consideration. We are a privately held corporation and do not release detailed financial statements – will you accept a Supplier Qualifier Report from Dun and Bradstreet?

A. Yes

Q. Page 13, Public Information Act. Will you accept a separate redacted proposal for any Public Information Act requests?

A. Any and all information submitted to EHN is subject to disclosure

Q. Is HUB subcontracting a requirement?

A. No

Q. Is an assessment of the HIPAA Breach Notification Rule (45 CFR §§ 164.400-414) in scope for this project?

A. Yes

Q. When was your last assessment of this nature performed?

A. 2019

Q. For how long should our proposal's pricing remain valid?

A. 90 days

Q. The Technical Information and Infrastructure Requirements in the Summary of Proposal section of the RFP (page 8) references a software solution. Should we submit our technical approach in this section?

A. Not Applicable

Q. Is Appendix A supposed to be the first page of the proposal after the transmittal letter and executive summary, or should it replace our cover page?

A. Cover letter as a first page is acceptable. Appendix A or Signature Page is the first page of your proposal.

Q. For Appendix F, are we supposed to submit a signed copy, or provide a statement acknowledging it?

A. This Appendix is for proposer information only, no response required

Q. Are there any anticipated COVID-19 impacts to the on-site component of this project?

A. No

Q. What prompted Emergence Health Network (EHN) to initiate the current request for HIPAA Security and Privacy assessment services?

A. EHN completes a Security and Privacy Assessment annually

Q. When does EHN prefer to initiate the HIPAA assessment activities? What is your anticipated timeline to conclude the assessment?

A. 4th Quarter of 2020 Calendar year.

Q. Does EHN want to have team members shadow our assessment team to learn and understand the assessment process to help establish skills for future self-assessments?

A. Yes

Q. Has EHN taken an enterprise approach to definition and documentation of HIPAA policies and procedures?

A. Yes

Q. Are HIPAA policies and procedures documented separately for outpatient clinics and the residential facilities?

A. No

Q. Has the organization experienced a HIPAA Privacy or Security breech event of greater than 500 records in the past 2 years?

A. No

Q. Does EHN leverage any HIPAA online or application tools to manage compliance?

A. Yes

Q. In the scope, you quote *164.502(b) Standard: Minimum Use and Disclosure of PHI*, however, 164.502(b) only covers Minimum Necessary. Do you intend to include 164.502(a) standard as well to cover general disclosure, or will it be restricted to Minimum Necessary?

A. This was an oversight, it will include both; 164.502(a) standard and 164.502(b) standard

Q.Is EHN looking for this project to provide a gap assessment against the in-scope requirements, or is EHN looking for a risk assessment to be conducted to satisfy the required implementation specification of 164.308(a)(1)(ii)(A) - Risk analysis (Required)?

A. We are looking to have the Required risk analysis completed.

Q.References to penetration testing and vulnerability scanning are made in the scope sections; is EHN looking for the vendor to quote those services or just provide reviews of these services that were previously performed by another vendor or in-house?

A. Selected vendor will be required to provide those services.

Q.Have there been risk assessments of any kind performed in the past? If so, are those results available for review?

A. Yes

Q. Do you have an updated data and asset inventory that identifies locations of ePHI?

A. Yes

Q. Will this report be used for internal purposes only?

A. No

Q. Do you use any third-party data hosting facilities?

A. Yes

Q. You request a qualified opinion of whether the identified risks are appropriate for an organization of your size, type, complexity. To ensure we have the same definition of opinion, are you looking for a formal auditor's opinion, issued under applicable AICPA attestation standards?

A. No

Q. Has cyber insurance been obtained?

A. Yes

Q. Does EHN have formal and mature incident management policies and processes in place?

A. Yes

Q. Does EHN employ any outside parties/legal counsel for potential security breaches (as part of incident management/business continuity)?

A. Yes

Q. Please confirm whether email submission is accepted in lieu of hard copy submission, or whether email submission is required in addition to hard copy submission.

A. Either hard copy or email

Q. On page 7 of the RFP, the Transmittal Letter is listed as Section II; please confirm what section should be entitled Section I.

A. Disregard "In Section II of the proposal, the" wording. Should be "Proposer must submit a transmittal letter that accomplishes the following:"

Q. Can the assessment be completed remotely via videoconferencing?

A. Penetration testing and interviews can be done remotely and 3 site visits at different locations.

Q. Beyond state requirements, are there any additional requirements that Emergence Health Network has due to the ongoing pandemic?

A. Yes, must follow CDC personal protective equipment guidelines

Q. Has Emergence Health Network completed a risk assessment previously?

A. Yes

Q. 15th bullet point on page 5 states "Contractor will conduct a second, and final penetration test and review updated report for management responses". Please elaborate on this. For example, a penetration test is similar to a vulnerability test but more intense. Would you like a 2nd external/internal vulnerability assessment to validate corrective action?

A. Yes

Q. Roughly how many management and staff are expected to be interviewed for each of the following:

- **Clinical**

- **Administrative**
- **Finance**
- **Human Resources**
- **IT**
- **Compliance**

A. Looking for selected vendor to guide the process.

Q. How many policies and procedures will need to be reviewed or rough estimate on the overall number of pages?

A. All necessary to complete the HIPAA Privacy and Security Risk Assessment

Q. For the physical security review, will just the three sampled sites be in scope? If additional sites are to be reviewed, how many locations?

A. Yes, 3

Q. Do you require vulnerability scanning and penetration testing or are we just evaluating the current practices?

A. Yes, vulnerability scanning and penetration testing.

Q. If vulnerability scanning and penetration testing are in scope, will it be conducted against all systems listed in the RFP?

A. Yes

Q. How many external-facing IP addresses are in scope?

A. 6

Q. Is wireless penetration testing required? If so, how many networks and access points will be tested?

A. Yes, 3 sites

Q. How many vendors or BAA's are expected to be reviewed?

A. 1 template

Answers to questions not answered on this document will be provided to the awarded vendor