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

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

ADDENDUM

To: All Interested Proposers

From: Diana Billingsley

Date: April 24, 2017

Subject: **HIPAA Security Risk Analysis RFP #17-009 Addendum I**

This addendum includes responses to all questions submitted as of Monday, April 24, 2017.

Any questions or additional information required by interested vendors must be emailed to bidquestions@ehnelpaso.org . RFP number and title must be on the "Subject Line" of the email. Attempts to circumvent this requirement may result in rejection of the proposal.

RFP No. 17-009
HIPAA Security Risk Analysis
Q&A

The queries raised by the bidders via subsequent emails up till April 24, 2017 and clarifications with regard to bid documents for the procurement of HIPAA Security Risk Analysis services are given as under:

Question Raised	Reply/Clarification
How many external facing assets/ IPs?	12
Is the network centralized? Can we access all assets from a single location?	Centralized at 210 E. Main, El Paso, Texas 79901
How many data centers do you have and where are their locations?	1- 210 E. Main, El Paso, Texas 79901
Outside of the administrative office, are we conducting full data collections at any of these locations, or just walking tours to validate adherence and observations?	Walking tours
Are security policies and procedures centralized? If not, describe.	Yes, using PolicyTech from Navex Global.
Is management of the security program and day-to-day activities centralized? If not, describe.	Yes, managed by the Health Information Technology division at EHN.
Do you have any Merger& Acquisition activity that is pending that could affect the scope?	Yes, one acquisition is pending.
If you have physician group (s), are they in scope for visits?	N/A
If you operate a health plan, is it in scope?	N/A
Are privacy policies and procedures centralized? If not, describe.	Yes, using PolicyTech From Navex Global.
How are privacy resources positioned across the organization and what is the reporting structure?	All privacy matters are centralized with the Privacy Officer, the Administrative Director of Health Information.
How many privacy FTEs (dedicated)?	1
For the review of the Business Associate Agreements are you wanting a review of the template that is used or a review of each of the BAAs you currently have? If so, how many are in need of review?	The template.
What is the approximate date vendor selection will be made?	30-60 days
How soon thereafter are services to be started (pending now delays or changes)?	30 days
Is there any written response needed to formally state our intentions to respond and submit a proposal?	No.
Is there a HUB participation requirement for this solicitation?	No requirement.
Section A, Project Description/Scope of Work: In this section the requested work is called a "security risk analysis"; however, from the description of requested work, it appears that EHN is requesting a HIPAA security "gap analysis" (i.e., a review of existing controls at EHN in comparison to required HIPAA Security Rule requirements/standards). Because there is a significant difference between performing a risk assessment/analysis versus a gap assessment/analysis, can EHN confirm that they desire a gap analysis?	EHN is in need of a Security Risk Analysis.
Section A, Project Description/Scope of Work: This section states that the contractor is required to produce an "audit report". Use of the term "audit" generally means performing an attestation engagement in accordance with	Attestation engagement audit, Government Auditing Standards, or AICPA standards are not part of the HIPAA Security Rule. After completion of the Security Risk Analysis the contractor should produce a detailed report of the findings that address all the areas applicable to the HIPAA Security

specific professional standards such as Government Auditing Standards or AICPA standards. Can EHN clarify whether expectations are that the requested work will be performed as an audit in accordance with audit/attestation standards, and if so, what audit/attestation standards?	Rule (administrative, technical, and physical safeguards, Security Rule Policies, assessment of vulnerabilities and threats, threat matrix, risk matrixes, recommended corrective actions, etc.).
Section A, Project Description/Scope of Work: This section states that the contractor assess physical safeguards. *a. Does EHN expect that all facilities (for example, the administrative office, 8 outpatient clinics, and 5 residential facilities) would be in-scope for the assessment of physical safeguards, or does EHN expect physical safeguards to be assessed just for the location housing its primary computing resources?* *b. If EHN expects assessment of physical safeguards at all facilities (which would require on-site visits to all facilities), can EHN provide the physical addresses for all facilitates?* *c. Are EHN's primary computing resources (i.e., the servers referenced) located in a central data center? If so, where is it located, and is it operated and managed by EHN IT staff?*	No, 3 sites are to be assessed. EHN Administration Offices Chase Tower Downtown 201 E. Main St. Suite 600 El Paso, TX, 79902 Central Outpatient/Extended Observation Unit/Crisis Emergency Services 1601 E. Yandell/1600Montana El Paso, TX, 79902 East Valley Outpatient 2400 Trawood Suite 301A El Paso, TX, 79936 Data center is located at EHN Administration Offices, Chase Tower Downtown, 201 E. Main St. Suite 600, El Paso, TX, 79902; EHN's data center is managed by EHN IT staff.
Section A, Project Description/Scope of Work, "EHN requires the following": In this list, the fourth bullet states "Review of Privacy Policies and Procedures". Does EHN expect that these policies and procedures would be assessed against the HIPAA Privacy Rule requirements (which would not normally be part of an assessment against the Security Rule)?	No
Section A, Project Description/Scope of Work, "EHN requires the following": Can EHN clarify the expectations related to the 15th bullet, "Support Development of a Risk Management Plan? Does EHN expect the contractor to assist in developing a Plan? If so, estimating the level of effort to do so would be very difficult without knowing what risks or compliance gaps will be identified, and including such support in an eight week timeline would be very difficult	Yes, assistance with the development of plan is part of this request for proposal. The plan would be completed after the completion of the Security Risk Analysis. The eight week timeline is for the completion of the Security Risk Analysis and presentation of the findings to the executives and board.
Section A, Project Description/Scope of Work, "EHN requires the following": Regarding the 12th bullet, "Security Risk Analysis Final Report is Completed Within 8 Weeks": *a. When does EHN expect this work to start?* *b. Does EHN have any flexibility related to the eight week deadline for completing the requested work?*	 Upon execution of the contract. Yes
Section A, Project Description/Scope of Work, "EHN requires the following": Regarding the last two bullets:	

a. Does EHN expect the presentations to be conducted on the same day or on two different dates? *b. Does EHN expect the presentations to be conducted in person (i.e., face-to-face rather than via teleconference)?*	The presentation needs to be given to the executive group first with at least 10-30 days apart to the board presentation. The executive presentation can be done via teleconference and the board presentation in person at EHN Administration Offices.
Section B, Proposal Requirements, Executive Summary, Item c. "Legal Proceedings": Can EHN clarify what information they desire related to this item?	Does the proposer have any pending legal proceedings.
Section B, Proposal Requirements, Qualifications and Scope of Services and Deliverables: EHN requests Project Methodology and Project Approach, respectively. These two topics appear to be the same or similar. Can EHN clarify what information they desire for each of these items?	Project Approach: General for the contract Project Methodology: Define, plan, launch, manage, and close. Project Approach in specific to conducting a risk assessment.
Section B, Proposal Requirements, Scope of Services and Deliverables: EHN requests "Methodology for conducting risk assessments". Similar to our question #1 above, the requested work appears to be for a gap analysis; therefore, can EHN clarify: *a. Whether a "risk assessment" or a "gap assessment" is desired?* *b. How this item (b.) is different than the proceeding item (a.) – "Project Approach"?*	Risk Assessment Project Approach: General for the contract Project Methodology: Define, plan, launch, manage, and close. Project Approach in specific to conducting a risk assessment.
Section B, Proposal Requirements, Cost Estimate: *a. Can EHN clarify what is meant by "for each element in the Scope of Work" in the context of the request that the contractor itemize fees? (For example, are the elements Conduct a security risk analysis; Produce a report; and Provide recommendations?) Or, are there another specific listing of elements for which EHN desires itemized fees?* *b. Can EHN clarify what is meant by "standard plan" in item c?*	Hourly rates per labor category or element based on the elements of your Security Risk Analysis. Do you have a standard plan for conducting Security Risk Analysis.
Section B, Proposal Requirements, References: For the requested references, the RFP requests references for 3-5 "companies". We perform services for only government entities, would EHN accept reference for 3-5 government entities for whom we have provided similar services?	Yes
Section B, Proposal Requirements, Forms / Attachment B, HUB Subcontracting Plan: If we do not plan to subcontract any of this work, do we need to complete this form? If so, is there someone at EHN that we can contact for guidance to ensure that we complete the form correctly?	If it does not apply; no.
Does EHN have an established budget for the requested work that can be shared with us?	There is no established budget at the moment for this request.
Understanding a due date of May 2nd for this RFP, I'm curious to know if there is a defined award/selection date, a start date (concerning year 1 activity) and a desired end/conclusion date (again, concerning year 1 activity). I thank you in advance for your response.	No. EHN will inform the preferred start date range when the final selection is made.
Is the respondent required to use NIST 800-53 as the guiding standard? Or is ISO/IEC 27001-2013 acceptable?	Either is acceptable as we did not specify.
The RFP states in the Notice to Interested Parties that "questions must be submitted by April 25th at 12:00	

MST," but also states that "questions regarding the specifications or proposal procedures must be received by EHN no less than 72 hours prior to the time set for proposal opening" (General Provisions #5). *a. Could you please specify which is the deadline for questions to be submitted?* *b. b. It is our policy to deliver proposals prior to the due date to avoid any delivery mix-ups or other events beyond our control related to mail. With questions due potentially less than a week before the due date, would the EHR consider an extension of the due date of at least a week to allow time for EHN to answer all questions, and for the proposer to review the Q&A and incorporate subsequent changes to the response?*	Deadline for questions is April 25, 2017 by 12:00 p.m. MT; the 72 hour deadline is for any protest regarding the specifications of the bid. At this time, unfortunately, we are not extending the due date.
Will the EHN accept submission of the proposal via email by the due date and allow the hardcopy of the response to follow one day after the due date, if EHN cannot extend the overall deadline?	Yes. Electronic submissions to the rfp email, however have to be received prior to 3:00 pm MT on the due date.
Reference the Conflict of Interest Questionnaire. If no employee of our firm has a business relationship with the local government entity (EHN or El Paso), do we need to include this signed form in our response? If we must include the form even if we have no relationships, is it EHN's expectation that we would enter "none" or "not applicable" in blocks 1 and 3?	Form must be signed with a N/A statement.
GENERAL LIABILITY: *• $500,000 – Fire Legal Damage Liability Emergence Health Network named as.* *o doesn't carry this.* *WORKERS COMPENSATION:* *• $1,000,000 – Employers Liability – Each Accident* *o Currently carrying $500,000.00.* *• $1,000,000 – Employers Liability – Each Employee* *o Currently carrying $500,000.00.* *• $1,000,000 – Employers Liability – Disease – Policy Limit Statutory Limits* *o Currently carrying $500,000.00.* *Would you kindly alert if our current position is acceptable or, if amends are required in lieu of disqualification*	Please submit what your current coverage is; this is not a disqualifier.
Page 6, Section 2 – Provide a summary of at least three comparable project *o To date, has not been engaged to conduct a HIPAA Risk Assessment as a standalone service offering. However, has been engaged for several data breach incident response projects and a single Information Systems Security Audit project where HIPAA Security Standards were audited and analyzed to varying degrees as part of the larger effort. has also conducted internal HIPPA Risk Assessments as part of our ongoing effort to be maintain certification as a HIPAA compliant organization. Please confirm that this similar experience,*	Yes, please elaborate in your response.

to be elaborated upon in our response,	
Page 7 – Provide references from 3-5 companies to whom we've provided the services being solicited within this RFP *o As noted above, is unable to provide references for the specific services being requested here as a standalone service offering. Please confirm that providing a minimum of 3 references from the similar project types discussed above qualifies as an applicant for this RFP, or justifies a waiver of this requirement.*	Please submit what you deem most appropriate; it will be evaluated by the selection committee; they are not disqualifiers.
Page 9 – Proposers must have been in the business of providing services for a minimum of 5 years *o has been in the litigation support technology business for over 20 years. has also been in the Cyber Security business for 2.5 years. Cyber Security professionals have up to five years of experience each. During that 2.5 year period, has provided breach incident response and penetration testing services for EHN. Please confirm that this past performance and stated experience qualifies as an applicant for this RFP, or justifies a waiver of this requirement.*	Please submit what you deem most appropriate; it will be evaluated by the selection committee; they are not disqualifiers.
How many data centers do you have?	1- 210 E. Main, El Paso, Texas 79901
Is there a subcontracting requirement to utilize Historically Underutilized Business (HUB)? If yes what is the minimum required %?	No there is no requirement.
What is HUB-LOI? (Found on Attachment B (HUB-LOI IS USED BY POTENTIAL VENDOR/VENDOR TO IDENTIFY SUB-VENDORS SELECTED FOR WORK ON THE CONTRACT)	Historically Underutilized Businesses- Letter of Intent
What is expected in Section 1. C. Legal Proceedings?	Does the proposer have any pending legal proceedings.

In case of any further information/clarification, they may send email and ask through bidquestions@ehnelpaso.org, individual visits are not entertained before April 25, 2017.