



Shelby County Tennessee

Mayor

Mark H. Luttrell, Jr.,

Questions & Answers

Issued: August 23, 2013

RFP #14-008-11 HIPAA & HITECH ACT COMPLIANCE CONSULTING SERVICES

TO ALL PROSPECTIVE BIDDERS:

The following questions were submitted by potential vendors

:

Question Number	Question	Response
1	Can a mixture of years of HIPAA, HITECH experience and years of risk assessment and compliance services on a similar scale be used to meet the minimum requirements	We request the experience be 5 years providing risk assessment services with similar entities for the purpose of HIPAA and HITECH compliance.
2	The Shelby County Government Website addressing EOC compliance indicates " To receive an EOC Contract Compliance Eligibility Number the following steps must be taken at least 45 days prior to bid opening. " RFP #14-008-11 was released August 9, 2013 and the proposal is due August 30, 2013. Are we still able to bid and be considered for selection given the EOC office stipulates the request for a vendor number needs to be made 45 days prior to bid opening?	Please go ahead and complete the vendor registration and EOC Compliance as outline in the RFP as a part of doing business with Shelby County Government.

3	Are Inmate Medical Services and their Business Associates included?	Inmate medical services are not included in the scope of this request however, components of the HER/EMR are hosted by SCG ITS and will be included in the assessment.
4	What kind of electronic health records (EHR) or electronic medical records (EMR) system is being used?	Currently a NexGen EMR is in use for inmate medical services, and a proprietary system named PTBMIS (State of Tennessee Health Department information system) are in use. Additional PHI and ePHI exist in multiple other file formats. A primary requirements of this engagement will be to discover the location and use of PHI and ePHI within SCG and to perform a Risk Assessment to determine the compliance state of all of it.
5	What organization or vendor maintains your EHR or EMR and what are the interfaces?	SCG ITS hosts the NexGen system with a third party company providing interface and software support. The PTBMIS system is supported by SCG ITS and the State of Tennessee. Again, these are not the only sources of PHI and ePHI and a primary purpose of this engagement is to discover additional ePHI and PHI within SCG.
6	Has Shelby County declared " Hybrid Entity " status? If so how many Covered Entities are designated?	There are currently three known departments of SCG with one of them having been declared a hybrid entity. SCG in total has not been declared a Hybrid entity.
7	Given the possibility of a large number of threats and vulnerabilities given the size and scope of your organization this requirement could generate a huge amount of detail that may not be useful and could drive up the cost? Would the buyer consider an alternative or a comprise?	This is the approach we have selected for this engagement.
8	At how many locations will site visits be required and where are these sites located?	The exact number of sites needing review is not currently know. There are something more than 60 offices and departments, many with multiple locations. Exact locations needing review will be dependant upon the results of initial discovery of PHI and ePHI use with the County.

9	How many staff member interviews will be required?	The exact number of staff interviews required will be dependant upon the results of initial discovery of PHI and ePHI use with the County.
10	Are any of the documents listed available online or will they be provided in hard copy?	Documents provided will be a mix of digital and hard copy.
11	Please clarify what exactly is being requested from Responders in the Cost Proposal? Is the requirement for a FFP or T&M contract?	We are seeking fixed price proposals.
12	What are the major line-of-business (LOB) applications used to create, receive, maintain, or transmit PHI?	Other than for the three known CEs, the LOBs for other County offices and departments are unknown as use of PHI and ePHI are not known and their determination is a requirement of this engagement.
13	What is the number and size of networks used or its branches/programs to create, receive, maintain or transmit PHI?	This knowledge is one of the anticipated results of this engagement.
14	Can you provide the number of systems included in the scope for the Gap Analysis and Risk Assessment so that we can develop a price quote?	This number is anticipated to be a result of the initial GAP analysis.
15	Approximately how many separate offices and departments are within the SGC?	There are approximately 68 offices and departments in SCG. Review of http://www.shelbycountyttn.gov/index.aspx?NID=8 will assist with understanding of the scope of this engagement.
16	Approximately how many separate offices and departments within the SGC currently use PHI and ePHI?	This will be determined by the selected vendor.
17	Approximately how many servers do you have that process ePHI?	This will be determined by the selected vendor.
18	Do you use a mainframe to process any ePHI? If so, what type?	Yes. There is one AS400 system known to process ePHI. There may be additional systems as well. The determination of additional systems will be determined by the selected vendor as part of this engagement.
19	How many system users do you have?	Approximately 5,300.
20	How many workstations do you have?	Approximately 5,300.
21	Do you use wireless networks?	Yes.

22	How many physical county offices are there?	Several offices and departments have multiple locations. The exact number requiring on-site review are unknown as we anticipate this list being a product of initial interviews and discovery.
23	How many computer applications does the SGC consider in scope to this project?	Currently all applications are in scope until eliminated from consideration through the discovery process.
24	Do you want the vendor to conduct vulnerability scans against the devices that process ePHI? If so, how many devices do you want scanned? We need to have the number of devices so we can determine the cost of conducting the scans.	Quantifying the devices requiring scanning is an expected output of this engagement. The actual scanning is not within the scope of this request.

Question Number	Question	Response
1	Are the consultants required to be onsite for this project?	Given the size of this engagement and the required results, it is anticipated that the selected vendor should anticipate the need to spend time onsite for this project.
2	Please describe current Information Security Policies. Is there one set of policies, and what is the approximate size? Are policies mapped to any particular control requirements (i.e. ISO 27001/27002, HIPAA or other)? Please describe total number of documents and approximate page count.	Descriptions can only be provided for the three currently identified CEs. There are currently multiple sets of policies and procedures which vary from being focused on HIPAA and PCI with additional Standard Operating Procedures in place. Based upon the unknown total quantity of CEs we will not provide the requested estimates.
3	For the purpose of Risk Assessment, how many areas of organization will be in scope? Entity-wide, specific business unit(s), specific process or application? Please describe.	One goal of this engagement is for the vendor to identify locations and usage of PHI and ePHI within Shelby County Government as a whole. The list of SCG departments is contained under the three community resources links on this URL, http://www.shelbycountyttn.gov/index.aspx?NID=8 . Until this is determined, specific processes and applications cannot be identified.

4	<p>For each area of the organization, please list key applications, systems and data repositories. Please note applications and systems that contain EPHI, and would negatively affect the organization if they were compromised in any way.</p>	<p>One goal of this engagement is for the vendor to identify locations and usage of PHI and ePHI within Shelby County Government as a whole. The list of SCG departments is contained under the three community resources links on this URL, http://www.shelbycountyttn.gov/index.aspx?NID=8. Until this is determined, specific processes and applications cannot be identified.</p>
5	<p>What is the primary EHR/EMR system (if applicable)?</p>	<p>The primary known HER/EMR system is a NexGen product. Again, it will be a primary purpose of this engagement to discover any additional systems in use within SCG.</p>
6	<p>How many individuals would need to be interviewed to understand the current controls on the above-listed systems, applications and processes? Please describe their job functions (i.e. IT, Compliance, Legal, HR, Business Data Owners).</p>	<p>We are unable to provide a complete estimate as subsequent interviews will be dependant upon the results of initial interviews. We anticipate at a minimum each SCG Department being interviewed after work with SCG ITS has been completed to finalize the project plan.</p>
7	<p>Will the Risk Assessment include aspects of Administrative, Technical and Physical aspects? In other words, are all control areas within scope?</p>	<p>Yes, all controls will require review.</p>
8	<p>As part of the Risk Assessment, is it desired that an OCR pre-audit be conducted, using the OCR Audit Protocol?</p>	<p>The OCR pre-audit is not sepcifically requested.</p>
9	<p>As part of the Risk Assessment, is it desired that Meaningful Use testing be conducted using the NIST approved test procedures for meaningful use as defined in 45 CFR §170.302(o) through (v)?</p>	<p>Meaningful Use Testing is outside of the scope of this engagement.</p>
10	<p>How many physical sites are in scope? Please list (at a minimum) data centers and locations for interviews with process owners. For hospitals and healthcare systems, please list any physician's practices and clinics that are within scope.</p>	<p>There are two primary SCG ITS data centers however, several offices and departments within SCG maintain seperate IT shops. One goal of this engagement is for the vendor to identify locations and usage of PHI and ePHI within Shelby County Government as a whole. The list of SCG departments is contained under the three community resources links on this URL, http://www.shelbycountyttn.gov/index.aspx?NID=8 with the vast majority of locations being available from the office and department pages. The discovery process may uncover additional locations requiring review.</p>

11	Is there any method in place to determine the value of Assets (i.e. data, applications, systems)? For instance, has your company conducted a Business Impact Analysis (BIA)?	A Business Impact Analysis has not been conducted for all potential CEs as they have not been identified. One goal of this engagement is for the vendor to identify locations and usage of PHI and ePHI within Shelby County Government as a whole.
----	--	---

Question Number	Question	Response
1	Section VII (a) in the RFP states that the scope of the activities will include “all Offices and Departments of SCG.” Can you please provide a list of all offices and departments for which assessment activities will need to take place?	One goal of this engagement is for the vendor to identify locations and usage of PHI and ePHI within Shelby County Government as a whole. The list of SCG departments is contained under the three community resources links on this URL, http://www.shelbycountyttn.gov/index.aspx?NID=8 .
2	To help quantify the scope and level of effort to perform the requested activities, can you please provide some additional details as to the current list of covered entities and business associates at SCG?	The current list of covered entities is limited, consisting of 3 office or departments of SCG.
3	Are the Shelby County Fire Department and Sheriff’s Office in-scope for this project?	Yes.
4	Can you provide details around the current HIPAA compliance ownership model at SCG? For example, has a privacy and security official been designated in each covered entity or are these responsibilities managed as a centralized function?	Privacy and Security officials have been established for Offices and Departments known to be Covered Entities. The model is decentralized with a central advising body under the mayor's administration which has members from the known CEs. As mentioned a primary need being filled in this request is the determination of CE status for SCG Offices and Departments.
5	Can you please provide details about the SCG Information Technology department including the number of employees and whether the department is centralized or decentralized?	Shelby County Government (SCG) Information Technology Services (ITS) consist of approximately 100 employees located primarily in two locations. SCG ITS provides centralized support to the Mayors Administration and support for several other SCG Offices and Departments ranging from complete IT services to provision of email only. Part of the output requested from this engagement is the determination of all Offices and Departments in SCG utilizing PHI or ePHI, and the

		current HIPAA compliance of each.
6	Has a HIPAA assessment, either Security Rule or Privacy Rule, been performed in the past two years? If so, will the awarded contractor be able to review the results of the prior year assessments?	While some assessments have been conducted in the last two years, the existence and status of assessments in most County offices and divisions is currently unknown. This is a component of the information we seek the vendor to gather and analyze as part of this assessment. Components of existing assessments, such as network diagrams, will be provided as required.
7	Would SCG prefer to have any anticipated travel costs estimated as a separate line item in the cost proposal or should travel costs be included in the total costs?	Travel costs should be listed as a separate line item and included in the total costs.
8	Has a budget been defined for this project and if so, would you be able to share those details?	A budget has been defined for this project. We are not permitted

Question Number	Question	Response
1	On the Shelby County Government website there are 69 total departments listed. Has a previous assessment been completed to determine the number of departments to be in scope of the HIPAA /HITECH assessment? If not, can you please share the expected or estimated number of departments that will be included in the scope of the assessment?	A Previous assessment has not been completed to determine the number of offices or departments which are in scope. Given the breadth of Shelby County Government (SCG) and the services provided, we are seeking to engage with a vendor who can determine which offices and departments are CEs. We are unable to provide an estimate as it may prematurely limit the scope leading to failure to identify all CEs within SCG.

2	How many departments that are expected to fall within scope of the assessment utilize a shared IT services department and how many in-scope departments have independent IT services (separate from the shared IT services)?	We do not have information concerning the total number of CEs within SCG who utilize shared or independent IT services. Of the currently identified CEs, 2 utilize shared SCG ITS services and the third is independent.
3	Are the key personnel for in-scope departments located on one central campus? If not, can you provide a list of departments by location?	Key personnel for possible in-scope departments are very likely not located on one campus. The vast majority of locations are available from the department information section of the SCG website. The discovery process may uncover additional locations requiring review.
4	How many current employees does Shelby County Government have?	Shelby County Government currently has approximately 6,100 active employees.
5	Page 23, Item 3 Cost and Fees: Does Shelby County expect all related fees / expenses (Hotel, meals, travel, etc.) to be included in total fees proposed or are you open to expense reimbursement?	We are seeking a proposal for total fees.

Robert S. (Bob) Brenner, Buyer
Purchasing Department
Shelby County Government

Cc: Bid File

