Request for Proposal
HIPAA Security Risk and Vulnerability Assessment

May 1, 2016

First Choice Community Healthcare
Timeline

The following Timeline has been defined to efficiently solicit multiple competitive proposals, select the most qualified vendor, and start the project within a short time period.

1. RFP Released to Vendors May 16th, 2016
2. Written Confirmation of Vendors intent to bid May 30th, 2016
3. Questions from Vendors About Scope or Approach June 3rd, 2016
4. Responses to Vendors about Scope or Approach June 10th, 2016
5. Proposal Due Date June 24th, 2016
7. Anticipated Decision and Selection of Vendor July 1st, 2016
8. Expected Project Start Date August 1st, 2016
9. Expected Deliverable Date August 26th, 2016

All proposals must remain valid for up to 30 days following the proposal due date. Any costs incurred during the development of this proposal or associated work will not be reimbursed.

Introduction

First Choice Community Healthcare is looking for a qualified information security assessment firm to perform a Security Risk Analysis (RA) as defined in the HIPAA Security Rule 45 CFR 164.308(a)(1)(A) and NIST SP 800 Special Publication 53. The RA will consist of both technical and compliance analysis of First Choice Community Healthcare IT infrastructure and security compliance program.

A. Definitions

- **Analysis** means the HIPAA Act Security and Privacy and NIST SP 800-53 Gap Analysis requested through this RFP
- **Compliance** means meeting the requirements of the HIPAA Security and Privacy Rules and NIST SP 800-53 guidelines.
- **Contract** means a written agreement between First Choice Community Healthcare and Responder selected to provide a HIPAA Security Risk and Vulnerability Assessment.
- **Consultant** means the successful Responder selected to provide a HIPAA Security Risk and Vulnerability Assessment contract to First Choice Community Healthcare.
- **ePHI** means electronic Protected Health Information
- **Gap Analysis** means an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by a covered entity. For the purposes of this RFP, gap analysis will also include a written report of analysis findings with short term and long term remediation necessary to ensure technical vulnerability findings are remediated or addressed, compliance with HIPAA Security and Privacy Rules and NIST SP 800-53, preparation of HIPAA Security and Privacy policies and procedures, staff and clinical areas have sufficient security training and knowledge and assistance in identifying covered components for an appropriate hybrid entity designation,
- **HIPAA** means the Health Insurance portability and Accountability Act of 1996
- **HIPAA Privacy Rule** means the provisions regarding the privacy of individually identifiable health information located in 45 CFR Part 160 and Subparts A and E of Part 164 as well as any amendments.
- **HIPAA Security Rule** means the provisions regarding security standards for the protection of electronic protected health information located in 45 CFR Part 160 and Subparts A and C of Part 164 as well as any amendments.
• PHI means Protected Health Information
• Proposal means a formal written response to this RFP submitted by a Responder.
• Request for Proposal (“RFP”) means all documents, including those attached or incorporated by reference, used for soliciting proposals to provide a HIPAA Security Risk and Vulnerability Assessment.
• Responder means any person or organization who submits a Proposal in response to this RFP.

B. The goals of this engagement are to:

1. Meet HIPAA Security Rule testing requirements.
2. Satisfy the Meaningful Use Core Objective to Protect Electronic Health Information.
3. Guide First Choice Community Healthcare’s Management team, specifically in Information Technology and Compliance, to more effectively prevent, detect, contain, and correct security violations.
4. Identify and detail areas of security risk within the First Choice Community Healthcare IT infrastructure, staff and the physical security of clinical and administrative facilities.
5. Gauge the effectiveness of First Choice Community Healthcare policies and procedures, including the execution of policies and response of staff and clinicians to a security event.
6. Develop a long term security partner relationship.

First Choice Community Healthcare is a community health system serving members in a three-county area of Albuquerque, New Mexico. This health center is a Health Center Program grantee under 42 U.S.C. 254b, and a deemed Public Health Service employee under 42 U.S.C. 233(g)-(n), and is accredited by the Joint Commission.

All proposals will be reviewed using the following criteria:

• Completeness of proposal
• Proven technical analysis capability
• Ability of deliverable to clearly communicate findings and recommendations
• Ability to identify the cause and effect of security risks across both compliance and IT, as well as specific training and response of First Choice Community Healthcare employees should a security event occur
• Demonstrated and verifiable information security experience in healthcare
• Vendor objectivity
• Proposal cost
• Ability of deliverable to satisfy timeline

Proposal bids should be submitted as a firm fixed price and an estimate for travel costs should be provided. First Choice Community Healthcare reserves the right to not select the lowest cost proposal and to not select a vendor if none sufficiently meet the goals of this RFP.

First Choice Community Healthcare will not be liable for any costs incurred by the vendor in preparing a response to this RFP. Vendors submit proposals at their own risk and expense. First Choice Community Healthcare makes no guarantee that any products or services will be purchased as a result of this RFP, and reserves the right to reject any and all proposals.
Proposal Requirements

A. Background

In 1996, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA), one of the purposes of which was to simplify and standardize the administrative functions of healthcare. The Administrative Simplification provisions (Title II) of this law require an adaptation and implementation of standards for the privacy, security and arrangement of electronic healthcare transactions. The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) of the American Recovery and Reinvestment Act of 2009 (ARRA) contains provisions that significantly affected the HIPAA Security and Privacy Rules. The HIPAA Privacy Rule and the HIPAA Security Rule (collectively, the “HIPAA Rules”) were issued by the United States Department of Health and Human Services in 2002 and 2003, respectively.

B. Purpose

In order to ensure compliance with the HIPAA Rules and NIST SP 800-53, First Choice Community Healthcare is requesting proposals for a Consultant to perform a HIPAA Security and Privacy Gap Analysis ("Analysis") for all First Choice Community Healthcare’s entities. The purpose of this RFP is to select a qualified Consultant to perform the gap assessment for all First Choice Community Healthcare infrastructure and facilities, identify problem areas and make specific recommendations for remediation to ensure HIPAA Security and Privacy compliance and compliance with NIST guidelines.

C. Summary of Scope of Work

The scope of work shall consist of visiting different First Choice Community Healthcare facilities and programs, including headquarters, to perform the compliance assessment, a technical vulnerability analysis of the internal and external IT infrastructure (including all servers, workstations, routers, switches and firewalls) and a remote social engineering assessment. A written summary of all problem areas shall include specific remediation recommendations for HIPAA Security and Privacy, and NIST SP 800-53 compliance. Additional deliverables, at First Choice Community Healthcare’s direction, may include a detailed project plan and support for remediating and addressing all findings, the drafting of organization-wide HIPAA Privacy and/or Security policies and procedures, and the development of a HIPAA Privacy and/or Security training program. The Consultant shall have the staff and resources to implement and complete the requirements of this RFP for the audit including the written summary due by [DATE TBD]. The timeframes for the additional deliverables may be negotiated.

Proposal Structure

The following sections will be included in the proposal, in this order:

1. Executive Summary – This section will present a high-level synopsis of the vendor’s response to the RFP. The Executive Summary should be a brief overview of the engagement, and should identify the main features and benefits of the proposed work and describe how the vendor solution addresses stated high level business and technical goals.

2. Company Overview – Provide a description of the company’s history, culture, number of years performing security assessments, relevant engagement experience, and key differentiators.

3. Fees – Itemize all fees associated with the project.
4. **Deliverables** – Include descriptions of the types of reports used to summarize and provide detailed information on security risk, vulnerabilities, and the necessary countermeasures and recommended corrective actions. Include sample reports as attachments to the proposal to provide an example of the types of reports that will be provided for this engagement.

5. **Schedule** – Include the method and approach used to manage the overall project and client correspondence. Briefly describe how the engagement proceeds from beginning to end and include payment terms. The vendor may propose a number of options for scheduling of the individual service options, including concurrent assessments where more accurate results may be generated.

6. **Contact Information** – Key sales and project management contact information including: name, title, address, direct telephone and fax numbers.

7. **References** – At least three healthcare clients where a similar scope of work was performed, within the past (18) eighteen months. References must include:
   - Organization name
   - Contact person and contact information (email, phone, address)
   - Services provided or performed for this client and length of service

8. **Team Member Biographies** – Include biographies and relevant experience of key staff and management personnel that will be involved with this project. Indicate if resources are employees of or sub-contracted by your organization.

9. **Scope and Methodology** – Detail specific objectives this scope will answer and reference frameworks, standards and/or guidelines used to develop scope. Also provide a detailed description of the methodology applied to complete the scope of work.

10. **Project Management** – a description and detail of the Vendor project management processes for facilitation of the engagement.

11. **Sample Reports** – Include as a separate attachment, sample reports of services to be provided.

**It is required for each proposal to completely address each section in this order to ensure a fair and accurate comparison of vendors.**

**Mandatory Requirements**

A. Conduct HIPAA Security and Privacy and NIST 800-53 gap analysis and prepare a written report of analysis findings for each branch/program that includes short and long-term remediation necessary to ensure HIPAA Security and Privacy compliance, compliance with NIST SP 800-53 guidelines, and generally-accepted security best practices.

The Responder shall:

1. Conduct a thorough Security Risk Analysis. The Analysis will specifically evaluate the current standing First Choice Community Healthcare’s business and clinical practices in relation to HIPAA Security and Privacy rules and NIST security guidelines. This will include current First Choice Community Healthcare’s operations and policy status as compared to HIPAA Security and Privacy Rule standard, NIST guidelines and generally-accepted security best practices, and specific remediation steps to correct potential violations. The Analysis will include all HIPAA connected First Choice Community Healthcare branch-
es/programs and related administrative policies and procedures, physical plant and office conditions, and information technologies in use by First Choice Community Healthcare.

2. Conduct a comprehensive technical vulnerability of the First Choice Community Healthcare IT infrastructure, to include both an internal technical vulnerability analysis and an external vulnerability and penetration assessment.

   a. The internal IT infrastructure vulnerability analysis should include:
      i. Systems analysis on the configuration of all servers and workstations
      ii. Network analysis for vulnerabilities with the network infrastructure, routers, switches and firewalls
      iii. Data security, including encryption of sensitive information, access and identity management to First Choice Community Healthcare network resources

   b. The external security vulnerability and penetration analysis should include:
      i. Network reconnaissance, employing passive and active gathering of data, to identify the network topology and potential areas of weakness
      ii. Enumeration of the network for analysis and identification of operating systems, services, protocols and configurations
      iii. Penetration analysis to attempt exploitation of identified and suspected vulnerabilities. The analysis should utilize both automated and manual processes.

3. Conduct onsite visits of various locations - to be determined by First Choice Community Healthcare - and programs in order to evaluate physical structures to determine if building or space modifications are required to comply with HIPAA Security and Privacy regulations or other state Security and Privacy statutes.

4. Interview selected management and staff members regarding common Security and Privacy related practices within branches/programs and between branches/programs to include, but not be limited to, disposal, storage, and encryption practices or procedures.

5. 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.

6. Evaluate the potential risks associated with how the different branches/programs collect, use, manage, house, disclose and dispose of information and evaluate options or changes to current practices in order to meet HIPAA Security and Privacy regulations or best practices for security of sensitive information.

7. Evaluate risks related to management, investigation and remediation of Security and Privacy breaches.

8. Assess and report on the response of selected First Choice Community Healthcare staff members to a simulated remote email and telephone phishing attack. The number of, and contact information for, the randomly selected employees will only be provided upon project initiation with the chosen vendor. The simulated email phishing attack may be conducted concurrent to the external vulnerability analysis at the discretion of First Choice Community Healthcare IT management, or via recommendation for scheduling by the selected vendor. Information on assessment attack vectors and methodology will be disclosed to First Choice Community Healthcare employees only by the CIO or designate, and on a strict need-to-know basis in order to maintain objectivity.

9. Analyze the current First Choice Community Healthcare physical and electronic PHI-handling and monitoring practices against the requirements of HIPAA Security and Privacy regulations and NIST SP 800-53 guidelines, and identify gaps between current practices and required practices under HIPAA Security and Privacy regulations and NIST SP 800-53.
10. Review First Choice Community Healthcare’s procedures for release, disclosure and recording of health information for compliance with each of the following HIPAA Security and Privacy standards:
   i. a. 164.308 Administrative Safeguards
   ii. b. 164.310 Physical Safeguards
   iii. c. 164.312 Technical Safeguards
   iv. d. 164.502(b) Standard: Minimum Use and Disclosure of PHI
   v. e. 164.530(a) Standard: Personnel Designations
   vi. f. 164.530(b) Standard: Training
   vii. g. 164.530(c) Standard: Safeguards
   viii. h. 164.530(d) Standard: Complaints to the Covered Entity
   ix. i. 164.530(e) Standard: Sanctions
   x. j. 164.530(f) Standard: Mitigation
   xi. k. 164.530(g) Standard: Refraining from Intimidating and Retaliatory Acts
   xii. l. 164.530(h) Standard: Waiver Rights
   xiii. m. 164.530(i) Standard: Policies and Procedures
   xiv. n. 164.530(j) Standard: Documentation

11. Review the First Choice Community Healthcare HIPAA Breach incident reporting and response practices, procedures and policies for sufficiency.

12. Review a sampling of First Choice Community Healthcare contracts, Business Associate Agreements and other organizational relationships for HIPAA Security and Privacy compliance.

13. Review First Choice Community Healthcare HIPAA Security and Privacy training modules currently used by the organization to determine if there are gaps between training content and HIPAA Security and Privacy standards or state Security and Privacy statutes. Evaluate training module to determine appropriate changes to improve training efficacy. Identify training requirements for staff, management, and executive levels to include determination if some training should be procured externally.

14. Review First Choice Community Healthcare’s Human Resources policies, procedures and practices for HIPAA Security and Privacy compliance, including the review of all HIPAA-related agreements for new hires (employees, contracted employees, temporary employees, volunteers, etc.), onboarding and termination procedures, the sufficiency of the HIPAA Security and Privacy Officers’ job descriptions and job assessments, employee disciplinary process and the protocol for addressing breach-related infractions.

15. Describe in detail a proposed analysis process to be followed for each branch/program including a work plan documenting tasks to be accomplished, timeframes and the responsible party.

16. Commence Analysis within thirty (30) calendar days of Contract award and complete Analysis within one hundred twenty (120) calendar days of the Contract award. Submit to First Choice Community Healthcare a comprehensive report detailing the findings of the Analysis, due within fifteen (15) calendar days (timeframe negotiable) of completing the field analysis.

17. Suggest specific short and long-term projects and remediation for each individual branch/program audited, including a tentative timeframe and budget, for the correction of identified discrepancies in HIPAA Security and Privacy compliance.
Deliverable

As a result of this project, First Choice Community Healthcare requests a documented and prioritized list of risks, each defined by a specific vulnerability, its impact, the asset affected, a rating of overall relative risk and criticality, references where applicable to specific regulations within the HIPAA Security and Privacy Rules and NIST SP 800-53, and a recommendation to mitigate the risk. The final report will consist of the following sections:

1. Executive Summary – appropriate for senior management to review and understand the current level of risk.
2. Introduction – including the scope and methodology used for this assessment.
3. Findings and Recommendations:
   a. Providing sufficient technical detail for the IT team to understand, replicate and remediate the issue.
   b. The findings for any compliance issues with HIPAA Security and Privacy Rules, NIST SP 800-53 and generally-accepted security best practices will include sufficient detail on remediation within First Choice business practices, workflows, policies and procedures.
4. Analysis Work Notes – documenting all control and/or vulnerability categories tested and the results of the testing.

The deliverable will be both concise and comprehensive, free from false positives and false negatives, and provide sufficient technical and compliance narrative detail to support all findings. Deliverable must be in PDF format and shall be delivered encrypted or via another secure method.

In addition, a presentation of findings to executive management and the technical team may be required.

Assessment follow-up access to the security engineering team for questions and clarifications is desired for a period of up to 12 months.

Contact Information

Proposal submission and all questions concerning this RFP, including technical and contractual, should be directed to the following person:

<table>
<thead>
<tr>
<th>Name</th>
<th>Jeffrey Cangialosi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Phone</td>
<td>505.924.9793</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:Jeffrey_cangialosi@fcch.com">Jeffrey_cangialosi@fcch.com</a></td>
</tr>
<tr>
<td>Physical Address</td>
<td>2001 N. Centro Familiar SW. Albuquerque, NM. 87105</td>
</tr>
</tbody>
</table>

Soliciting information about this RFP after the release date, from anyone within First Choice Community Healthcare (FCCH) other than the above listed person may forfeit the vendor. Vendors shall not contact any FCCH personnel during the proposal process without express permission of the FCCH representative listed above. FCCH may disqualify any vendor who has made site visits, contacted FCCH personnel or distributed any literature without authorization from the owner of this process.
All questions regarding this proposal and process should be directed in writing to:

Jeffrey Cangialosi (Chief Information Officer) at: jeffrey_cangialosi@fcch.com

Any proposal received after the required time and date specified for shall be considered late and non-responsive. Any late proposals will not be evaluated.