Request for Proposals
HIPAA Security and Privacy Audit and Gap Analysis

FIRST CHOICE COMMUNITY HEALTHCARE, INC.

RFP#17_002
August 2, 2017
I. Introduction

First Choice Community Healthcare, Inc. (FCCH) is seeking proposals to provide Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act Compliance and Consulting Services for all clinical and administrative facilities and activities at FCCH. This Request for Proposals (RFP) is to invite interested and qualified companies and professionals to submit proposals in accordance with the instructions provided where the successful Proposer will be invited to enter into a contractual relationship with FCCH for the services outlined in this RFP.

A. Definitions

- **Analysis** means the HIPAA/HITECH Act Security and Privacy Audit and Gap Analysis requested through this RFP.
- **Compliance** means meeting the requirements of the HIPAA Security and Privacy Rules.
- **Contract** means a written agreement between FCCH and successful Proposer to provide a HIPAA Security and Privacy Audit and Gap Analysis.
- **Consultant** means the Proposer selected to provide a HIPAA Security and Privacy Audit and Gap Analysis to FCCH.
- **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 recommendations necessary to ensure technical vulnerability findings are remediated or addressed, compliance with HIPAA Security and Privacy Rules, preparation and/or recommend updates to HIPAA Security and Privacy policies and procedures, and review of existing HIPAA Privacy and Security mandated training programs, and, if necessary, recommendations for enhancements to training programs.
- **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.
- **HITECH Act** means the Health Information Technology for Economic and Clinical Health Act of 2009 as well as any amendments.
- **PHI** means Protected Health Information for an individual that identifies past, present, or future health conditions or provisions of health care.
- **Proposal** means a formal written response to this RFP submitted by a Proposer.
- **Request for Proposal (RFP)** means all documents, including those attached or incorporated by reference, used for soliciting proposals to provide a HIPAA Security and Privacy Audit and Gap Analysis.
- **Proposer** means any person or organization who submits a Proposal in response to this RFP.
B. The goals of this engagement are to:

1. Identify and allow FCCH to better understand potential internal and external threats and vulnerabilities to our electronic data;
2. Compare FCCH’s existing security measures (both technical and policy/procedure-oriented) with the requirements of HIPAA’s privacy and security regulations;
3. Guide FCCH’s management team to effectively prevent, detect, contain, and correct HIPAA privacy and/or security incidences.
4. Identify and detail areas of possible HIPAA privacy and security risks within the FCCH’s information technology infrastructure, staff and clinical and administrative facilities.
5. Recommend feasible privacy and security measures that will allow FCCH to address policy issues, eliminate or mitigate harm resulting from each identified potential threat and vulnerability, and comply with HIPAA’s privacy and security regulations.

II. Timeline

The following Timeline has been defined to efficiently solicit multiple competitive proposals, select the most qualified Proposer and complete the analysis within the most expeditious timeframe.

1. RFP Released
2. Written Confirmation of Proposers’ intent to bid
3. Questions from Proposers
4. Responses to Proposers
5. Proposal Due Date
6. Proposal Review, Decision & Selection of Proposer
7. Contract Negotiation*
8. Expected Project Start Date*
9. Expected Deliverable Date*

* Tentative dates

All proposals shall remain valid for 60 days following the proposal due date. Any costs incurred by Proposers during the development of their proposal or associated work will not be reimbursed. Questions from Proposers are due no later than the date and time indicated above and must be submitted electronically to RFP@FCCH.COM and must include “Questions – HIPAA Security Assessment – RFP#17_002” in the subject line.

III. Organization

FCCH is a community health care system providing primary medical, dental, and behavioral health care services to the under-served populations of the Middle Rio Grande Valley of central New Mexico. FCCH has been in existence since 1972. The communities we serve lie within the Greater Albuquerque Metropolitan Statistical Area and include Bernalillo and southern Santa Fe and Valencia counties. Because of relatively few other health care providers, our service area also extends into adjacent Torrance, Socorro, and Sandoval counties. FCCH employs a staff of 460(+-) and provided care to 50,280 patients through more than 157,900 patient encounters in 2016. We operate a Cerner-based electronic medical records system, and a Dentrix-based electronic dental records system. FCCH 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.
IV. 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.

FCCH falls into the category of a “Covered Entity Provider” and as such must be compliant with all HIPAA and HITECH rules. FCCH has developed HIPAA Policies and Procedures to govern the handling of private and protected health information.

B. Purpose

In order to ensure compliance with the HIPAA Rules, FCCH is requesting proposals for the performance of a HIPAA Security and Privacy Audit and Gap Analysis for all FCCH clinical and administrative facilities and activities. The purpose of this RFP is to select a qualified Consultant to perform the audit/gap assessment for all FCCH infrastructure and facilities, identify problem areas and make specific recommendations for remediation to ensure HIPAA Security and Privacy compliance.

C. Summary of Scope of Work

The scope of work shall consist of visiting all FCCH clinical and administrative facilities to perform the compliance audit and analysis and an analysis of the internal and external IT infrastructure. A written summary of all problem areas shall include specific remediation recommendations for HIPAA Security and Privacy compliance. Additional deliverables, at FCCH’s direction, may include 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 possess the staff and resources to implement and complete the requirements of this RFP including the written summary pursuant to Section II. The timeframes for the additional deliverables may be negotiated.

V. 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 Proposer’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 Proposer’s solution addresses stated high level business and technical goals. The Executive Summary should also include the pricing structure.

2. Company Overview – Provide a description of the company’s history, culture, number of years performing HIPAA security audits/assessments, the number of employees, the number of years in existence, relevant engagement experience, and key differentiators.
3. **Fees** – Itemization all fees associated with the project including payment terms.

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.

5. **Schedule** – Include the method and approach used to manage the overall project and client engagement/correspondence. Briefly describe how the engagement proceeds from beginning to end. The Proposer 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 (e-mail, phone, address); and
   - 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, including a description of security certifications and accreditations relevant to HIPAA's privacy and security regulations.

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 Proposer’s project management processes for facilitation of the engagement.

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

12. A list of relevant articles, white papers, and any seminars conducted by the Proposer regarding compliance with HIPAA’s privacy and security regulations.

**Each proposal must completely address each section in this order to ensure a fair and accurate comparison of vendors.**

**VI. Services to be Provided**

Conduct a HIPAA Security and Privacy audit and gap analysis and prepare a written report of analysis/audit findings for each facility and activity that includes short and long-term remediation necessary to ensure HIPAA Security and Privacy compliance, OCR Phase 2 HIPAA Audit compliance, and generally-accepted security best practices.

The Proposer shall:

In general, conduct a thorough HIPAA Security and Privacy Audit and Gap Analysis. The Analysis will specifically evaluate the current standing FCCH business and clinical practices in relation to HIPAA Security and Privacy rules. This will include current FCCH operations and policy status as compared to HIPAA Security and Privacy Rule standards, OCR guidelines, and generally-accepted security best practices, and specific remediation steps to correct possible gaps and vulnerabilities. The Analysis will include all FCCH facilities and activities, related administrative policies and procedures, physical facility and office conditions, and information technologies in use by FCCH.

Proposers shall describe in detail a proposed analysis process to be followed for each facility/department program including a work plan documenting tasks to be accomplished, timeframes and the responsible party.
Proposers shall also suggest specific short and long-term projects and remediation for each individual facility/department audited, including a tentative timeframe and estimated cost, for the correction of identified discrepancies in HIPAA Security and Privacy compliance.

The following items are specifically requested. Please provide a cost for each numbered item. FCCH reserves the right to select some or all of the items.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Compare HIPAA Privacy and Security regulations with all New Mexico state security and confidentiality statutes and identify which state statutes are more restrictive than federal law.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Conduct a comprehensive audit and gap analysis of FCCH’s IT infrastructure. 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. Evaluate the potential risks associated with how facilities and activities collect, use, manage, house, disclose and dispose of patient health information and evaluate options or changes to current practices in order to meet HIPAA security and privacy regulations, OCR guidelines, or best practices for security of sensitive information.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Conduct onsite visits of all clinical and administrative facilities in order to evaluate physical structures to determine if building or space modifications are required to comply with HIPAA Security and Privacy regulations, OCR guidelines, or other state Security and Privacy statutes.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Interview an appropriate spectrum of management and staff members regarding common security and privacy related practices within and between clinical and administrative facilities to include, but not be limited to, disposal, storage, and encryption practices or procedures.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Evaluate risks related to management, investigation and remediation of HIPAA Security and Privacy breaches and review the FCCH HIPAA breach incident reporting and response practices, procedures and policies for sufficiency;</td>
<td></td>
</tr>
</tbody>
</table>
| 6    | Review FCCH procedures for release, disclosure and recording of health information for compliance with each of the following HIPAA Security and Privacy standards:  
  a. 164.308 Administrative Safeguards  
     1. Current risk analysis procedures and process;  
     2. Policies and procedures relevant to operational security including business associate security requirements;  
     3. Information access restrictions and controls;  
     4. Security awareness training; and  
     5. Incident response procedures and disaster recovery plan  
  b. 164.310 Physical Safeguards  
     6. Physical access controls including building access and appropriate record keeping;  
     7. Workstation security policies and procedures; and  
     8. Proper usage, storage, and disposal of data storage devices  
  c. 164.312 Technical Safeguards  
     9. Auditing and audit procedures;  
     10. Use of encryption devices and tools;  
     11. Implementation of technology to ensure electronic protected health |  |
information confidentiality, integrity and availability, including:

a. Internal/external network assessment;
b. Internet/intranet/extranet;
c. Network architecture;
d. Web applications and in-house developed applications;
e. Wireless networks;
f. Host diagnostics;
g. Firewall diagnostics; and
h. Virtual Private Networks

d. 164.502(b) Standard: Minimum Use and Disclosure of PHI;
e. 164.530(a) Standard: Personnel Designations;
f. 164.530(b) Standard: Training;
g. 164.530(c) Standard: Safeguards;
h. 164.530(d) Standard: Complaints to the Covered Entity;
i. 164.530(e) Standard: Sanctions;
j. 164.530(f) Standard: Mitigation;
k. 164.530(g) Standard: Refraining from Intimidating and Retaliatory Acts;
l. 164.530(h) Standard: Waiver Rights;
m. 164.530(i) Standard: Policies and Procedures; and
n. 164.530(j) Standard: Documentation.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Review a sampling of FCCH contracts, Business Associate Agreements and other organizational relationships for HIPAA Security and Privacy compliance.</td>
</tr>
<tr>
<td>8</td>
<td>Review FCCH HIPAA Security and Privacy training modules currently in use to determine if there are gaps between training content and HIPAA Security and Privacy standards or state security and privacy statutes. Evaluate training modules 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.</td>
</tr>
<tr>
<td>9</td>
<td>Review FCCH human resource 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.</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
</tr>
</tbody>
</table>

**VII. Deliverables**

FCCH requires 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 a recommendation to mitigate the risk.

The deliverables 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.

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

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 to include, but not be limited to, a summary of the scope, approach and recommendations.

2. Introduction – including the scope and methodology used for this assessment.

3. Detailed Findings and Recommendations -- providing sufficient technical detail for the IT team and/or facility staff to understand, replicate, and remediate the issue. Findings and recommendations shall include:
   a. A matrix of threats and vulnerabilities to FCCH’s electronic data, including probability and impact of each threat and vulnerability based on FCCH’s current privacy and security measures and Proposer’s recommended privacy and security measures;
   b. Supporting detailed exhibits explaining threats and vulnerabilities;
   c. A list of FCCH’s technical and non-technical deficiencies in comparison with the requirements of HIPAA’s Privacy and Security regulations;
   d. A detailed report of findings for compliance issues with HIPAA Security and Privacy Rules, OCR guidelines, generally-accepted security best practices; and recommended remediation measures for each identified threat, vulnerability and deficiency within FCCH’s business practices, workflows, policies, and procedures. The report should include estimated costs for each recommendation, broken down by cost for hardware, software, consulting services, etc.;

4. Analysis Work Notes – documenting all control and/or gaps and/or vulnerability categories evaluated and the results of the evaluation.

5. A milestone-based work plan with a recommended timeline to implement each recommended remediation measure.

A formal on-site presentation of findings to executive management and the technical team shall be required.

VIII. Proposal Evaluation

Proposals deemed responsive will be evaluated based on the proposal structure requirements listed in Section V and scored pursuant to the scoring matrix in Section IX. FCCH reserves the right to reject any and all proposals as non-responsive, and re-issue this Request for Proposals should the need arise. Proposals shall be valid for 60 (sixty) days following proposal due date as indicated in Section I above.

Interested firms must submit an electronic version of their proposal, detailing their qualifications along with their proposed project cost and hourly rates to RFP@FCCH.COM and must include “Proposal – HIPAA Security Assessment – RFP#17_002” in the subject line. Proposals must be received no later than 5:00 PM Mountain Time on the Proposal Due Date specified in Section II. Faxed proposals will not be accepted.

Proposals will be reviewed according to the following criteria:
- Completeness and clarity;
- Proposer’s experience with similar projects and proven capability;
- Proposal cost;
- Ability to satisfy stated timelines
- Personnel qualifications; and
- References.
FCCH reserves the right to negotiate the final scope of this project based, in part, on Proposers’ submitted costs for each deliverable. Estimated travel costs (if any) should be provided. FCCH reserves the right to waive any technical irregularities, to seek written clarification on proposals from any or all Proposers, to not select the lowest cost proposal and to select no proposals if none sufficiently meet the goals of this RFP. No clarification will be sought if the Proposer completely fails to address a feature contained in the RFP. If the failure was in response to a mandatory feature, the Proposer may be disqualified.

Upon completion of the evaluation process, FCCH intends to select a Proposer with whom to negotiate a contract, based on the evaluation findings and/or other such criteria as deemed relevant for ensuring that the decision is made in the best interest of FCCH. In the event FCCH is successful in executing a contract with the selected Proposer, FCCH will issue a notice of award. In the event FCCH is not successful in executing a contract with the selected Proposer, FCCH reserves the right to negotiate with another Proposer. FCCH may cancel this procurement and make no award, if such determination is deemed to be in FCCH’s best interest.

FCCH will not be liable for any costs incurred by the Proposer in preparing a response to this RFP. Proposers submit proposals at their own risk and expense. FCCH 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. Any proprietary material submitted in response to this RFP shall be so identified.

Soliciting information about this RFP after the release date, from anyone within FCCH may forfeit the Proposer. Proposers shall not contact any FCCH personnel during the proposal process without express permission of FCCH. FCCH may disqualify any Proposer who has made site visits, contacted FCCH personnel or distributed any literature without authorization from FCCH.

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.

**IX. Proposal Scoring**

Proposals shall be scored according to the following:

<table>
<thead>
<tr>
<th>Base Points Possible</th>
<th>Extra Points Possible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness and clarity of Proposal</td>
<td>Experience working with Federally Qualified Health Center systems</td>
</tr>
<tr>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Proposer’s experience with similar projects and proven capability</td>
<td>Small/ woman/ minority owned business</td>
</tr>
<tr>
<td>25</td>
<td>5</td>
</tr>
<tr>
<td>Proposal cost</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Personnel qualifications</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>References</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

**Total Base Points**

100

**Total Extra Points**

15

Please Note: a score of zero (0) on any scored item may cause the entire response to be eliminated from further consideration.
X. **Other Documents to be Submitted**

- Current W-9, Request for Taxpayer ID Number Certification
- Current NM CRS ID Number
- Business license
- Business Data for 1099 purposes

FCCH will verify that the selected Proposer does not appear on the US Department of Health and Human Services’ Office of the Inspector General’s Exclusion List prior to any contract negotiation.

XI. **Assurances**

The successful bidder must comply with all Federal statutes relating to nondiscrimination. These include, but are not limited to:

- **Title VI of the Civil Rights Act of 1964** (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin;
- **Title IX of the Education Amendments of 1972**, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex;
- **Section 504 of the Rehabilitation Act of 1973**, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; and