REQUEST FOR PROPOSAL

7750 East Broadway Boulevard, Suite A-200, Tucson, AZ 85710 • riskrfp@blake.easterseals.com

Easterseals Blake Foundation hereby requests bids for information security and regulatory compliance (e.g. HIPAA, FERPA) risk assessment services, while encouraging responses from qualified individuals and small and minority-owned firms, as follows:

RFP Item 1
HIPAA Privacy and Security Risk Assessment

Requirements & overview:

EBF has identified the following requirements for its HIPAA Privacy and Security Risk Assessment project.

It is noteworthy to highlight that EBF seeks a comprehensive risk assessment, not simply a technical risk assessment (e.g. vulnerability assessment, patch assessment) or review of the sufficiency of information technology controls.

Locations in scope:

- EBF's administrative offices located at 7750 East Broadway Boulevard, Suite A-200, Tucson.
- (1) Behavioral Health program clinical facility located at 7750 East Broadway Boulevard, Tucson, Suite A-100, whose operations are representative of EBF's other BH program clinical facilities across the State.
- (1) CFS program facility located at 7750 East Broadway Boulevard, Tucson, Suite C-200, whose operations are representative of EBF's other CFS program facilities across the State.

- (1) SAGE program employment facility located at 1010 North 5th Avenue, Tucson, whose operations are representative of EBF’s other SAGE program employment facilities across the State.
- (1) SAGE program clinical rehabilitation facility located at 4410 West Ironwood Hills Drive, Tucson, whose operations are representative of EBF’s other SAGE program clinical rehabilitation facilities across the State.
- (1) CLS program location to be determined, whose operations are representative of EBF’s other CLS program locations across the State.
- (1) SLS program location to be determined, whose operations are representative of EBF’s other SLS program locations across the State.

Tasks in scope:

1. Establish whether EBF is operating in compliance with HIPAA requirements, considering, but not limited to, each of the following HIPAA Privacy and Security standards:

    - 163.306 General Requirements
    - 164.308 Administrative Safeguards
    - 164.310 Physical Safeguards
    - 164.312 Technical Safeguards
    - 164.316 Policies, Procedures and Documentation
    - 164.502(b) Standard: Minimum Use and Disclosure of PHI
    - 164.530(a) Standard: Personnel Designations
    - 164.530(b) Standard: Training
    - 164.530(c) Standard: Safeguards
    - 164.530(d) Standard: Complaints to the Covered Entity
    - 164.530(e) Standard: Sanctions
    - 164.530(f) Standard: Mitigation
    - 164.530(g) Standard: Refraining from Intimidating and Retaliatory Acts
    - 164.530(h) Standard: Waiver Rights
    - 164.530(i) Standard: Policies and Procedure
    - 164.530(j) Standard: Documentation

2. Evaluate sampled locations to determine how and where PHI or ePHI is collected, used, managed, stored, maintained, disclosed, transmitted, and / or disposed of.

3. Assess the policies, procedures, and controls presently in place, and the effectiveness of those policies, procedures, and controls.

4. Evaluate and measure the net HIPAA compliance risk (remaining risk after the application of existing policies, procedures, and controls) associated with how PHI or ePHI is collected, used, managed, stored, maintained, disclosed, transmitted, and / or disposed of at sampled locations, whether physical or electronic. This evaluation should model and document the estimated cost of failure should the risk be exploited to result in a privacy or security breach.

5. Provide documentation that fulfills the risk assessment requirement of HIPAA and otherwise provides an admissible report for Federal and State audits. Contractor expressly waives any confidentiality or non-disclosure provision which prohibits disclosure of project deliverables.

6. Provide a prioritized list of realistic options for reducing identified risks. Each option should include an estimated cost and otherwise describe how it meets or contributes to regulatory compliance.

7. For “addressable” HIPAA specifications that are determined to be unreasonable or inappropriate for an organization of our size, type, and complexity, formally document why they are not reasonable or appropriate and / or the alternative security measures that are being implemented and how those alternative security measures enable the standard to be met.

8. Compare HIPAA Privacy & Security Rule requirements with EBF’s contractual requirements to identify any requirements which are more restrictive and the extent to which EBF meets the more restrictive requirement. This analysis shall reference primary sources.

Guidance relating to expected actions to deliver tasks in scope:

- Perform on-site visits to each of the in-scope locations to--
    - Interview a sample of management and staff.
        - Clinical
        - Administrative
        - Finance
        - Human Resources
        - Information Technology
        - Compliance
    - Evaluate actual clinical practices (e.g. interaction with patients, handling of PHI and ePHI) and compare those practices against written policies and procedures.
    - Evaluate actual non-clinical practices in clinical facilities (e.g. privacy in waiting room, intake areas) and compare those practices against written policies and procedures.
    - Evaluate physical security and the sufficiency of physical security controls.
- Whether on-site or off-site--
    - Evaluate policies and procedures relating to clinical operations.
    - Evaluate policies, procedures, and practices relating to information technology operations.
    - Evaluate policies, procedures, and practices relating to information security.
    - Evaluate information technology design architecture, in the following domains:
        - Wide area network.
            - A perimeter vulnerability assessment is not required unless it will exceed the capabilities of our presently contracted Qualys service.
        - Multifunction devices (e.g. printer, scanner, and FAX).
        - Servers and endpoints (e.g. desktop, laptop, tablet) infrastructure.
            - This evaluation should consider, but not be limited to, encryption, media access, user privileges, password practices, patching practices, anti-malware practices, and Active Directory Group Policy implications.

            - This evaluation should also consider physical security of devices.
        - Cloud solutions.
            - This evaluation should consider, but not be limited to, our cloud-based EHR/EMR solutions, and HRIS solutions.
        - Applications.
        - Local area network.
        - Disaster recovery.
        - High availability.
    - Evaluate telecommunications (e.g. telephones and mobile telephones) policies, procedures, and practices.
    - Evaluate policies, procedures, and practices relating to human resources on-boarding, management, and off-boarding of employees and contractors.
    - Evaluate policies, procedures, and practices relating to training (including security awareness) of employees and contractors, relating to their obligations under HIPAA.
    - Evaluate policies, procedures, and practices directly relating to compliance, including but not limited to:
        - Breach / incident reporting and response.
        - Business Associate Agreements use and sufficiency.
        - Regulatory mandates.

Project deliverables:

- A document that fulfills the risk assessment requirement of HIPAA and otherwise provides an admissible report for Federal and State audits, in the following format:
    - Executive Summary
        - Includes an overview appropriate for senior management to understand the current level of risk.
    - Introduction
        - Outlines the scope and methodology used to deliver the assessment.
    - Findings
        - Outlines the outcome of the risk assessment in specific detail.
    - Opinion

        - Provides an opinion of whether identified risk levels are appropriate for an organization of our size, type, and complexity.
    - Recommendations
        - Outlines the recommendations provided to reduce (or further reduce) identified risk.
    - Work Notes
        - All source materials and work notes used to create the report.
- Up to eight hours of conference time between the Contractor and EBF leadership, either in-person or by videoconference, within two weeks of having delivered the report, to discuss the findings.
- Contractor will initially provide a draft report, allowing for management responses. Management responses will be incorporated into, and made a part of the final report, without modification or prejudice.
- Contractor expressly waives any confidentiality or non-disclosure provision which prohibits disclosure of project deliverables.

RFP Item 2
Family Educational Rights and Privacy Act (FERPA) Risk Assessment Supplement

Supplement overview:

Expand upon the scope outlined in RFP Item 1, as follows:

- Evaluate (1) additional CFS program facility that operates as a child care and preschool providing academic and Head Start services regulated under FERPA, whose operations are representative of similar CFS program facilities across the State.

- Develop a supplement to the deliverable document of RFP Item 1 which outlines any FERPA compliance gap or gaps that would not otherwise be met by resolving the gap(s) already identified to

meet the more stringent HIPAA compliance requirements, together with recommendations that would resolve such gap(s).

- This supplement should be incorporated into the deliverable document with the chapter heading, “FERPA Compliance Supplement”

501(c)3 nature of Easterseals Blake Foundation

Easterseals Blake Foundation is a 501(c)3 non-profit social service agency. In-kind donations of services, or portions of services, may be eligible for a tax deduction equal to their fair market value. By extension, bidders may wish to consider “donating” a portion of their services, but should consult with a Certified Public Accountant before doing so.

Information Technology infrastructure:

The Easterseals Blake Foundation information technology infrastructure includes, but is not limited to, the following:

- (11) ASA-5505 firewall appliances used both as an internet gateway, and to sponsor VPN connections to the agency’s primary and disaster recovery locations from key remote offices.
- (2) ASA-5510 firewall appliances used both as an internet gateway, and to host VPN connections from key remote offices to the agency’s primary and disaster recovery locations.
- Approximately (700) endpoint devices (e.g. desktop, laptop, tablet).
- Approximately (421) cellular telephones.
- Various on-premise telephone systems at office locations, which are being transitioned to a cloud provider.
- Approximately (14) physical servers.
    - Microsoft Windows Server for file and print services.
    - Microsoft Terminal Services for remote access services.
    - Microsoft Exchange for e-mail and web-mail services.
- (2) Sophos SEA secure e-mail gateway appliances, one each at our primary and disaster recovery locations, used for e-mail risk management (e.g. data loss prevention, ePHI encryption, antivirus, antispam)
- (2) Ruckus SmartZone 100 wireless controller applications, one each at our primary and disaster recovery locations, used for wireless management and security (e.g. encryption, 802.1x authorization)

- (1) Dell PowerVault TL2000 tape library w/ (2) LTO-7 tape drives at our primary location.
- (1) Dell PowerVault LTO-7 tape drive at our disaster recovery location.
- HiMS cloud-delivered electronic medical record software
- PriSM cloud-delivered human resources software, used for payroll, etc.
- Mozy for online backup of certain systems.
- Microsoft Azure for online backup of certain systems.

Bid request 1:

- A fixed cost all-inclusive price to deliver RFP Item 1.

Bid request 2:

- A fixed cost all-inclusive price to deliver both RFP Item 1 and RFP Item 2.

Bid request 3:

- A fixed cost all-inclusive hourly rate, for each of the staff that will perform the assessment, should EBF choose to engage them during or following this assessment, for areas outside the scope of the RFP.
    - Bidder will honor this supplemental hourly rate for a period of (6) months following project completion.

A summary of each of the staff that will perform the assessment, and their qualification(s).

Submission details:

- Bidders that anticipate a submission should respond immediately and acknowledge their intention to riskrfp@blake.easterseals.com in order to receive any updates / supplements.
- Bidders with questions on this RFP or the EBF environment should submit them in writing to riskrfp@blake.easterseals.com.
    - Such questions and any responses will be collected and shared with all other bidders.
    - EBF shall adopt a ‘quiet period’ and refuse direct interaction with bidders outside of e-mailed question and answers, as described above.

- Submissions shall be delivered in writing to the Easterseals Blake Foundation office at 7750 East Broadway, Suite A200, Tucson, AZ 85710, or by email to riskrfp@blake.easterseals.com.
- Submissions are due no later than Friday, September 8 at 5:00PM.
- EBF anticipates award of this RFP by Friday, September 30th, however bidders shall honor their quoted pricing through to March 31, 2018.
- Bidders shall explicitly warrant that the project will be completed within (60) days of commencement, unless bidder can provide off-demand pricing that reflects a significant cost reduction for delivery delays.
- Bidders acknowledge that
    - Final payment will only be released when the full scope of project tasks (1 – 8) have been delivered, however EBF will consider progress payments.
    - The award of this project will be disproportionately based on the qualifications of the staff performing it, therefore substitutions of staff will not be permitted.

Qualifications:

- Bidders shall provide evidence of an active Commercial General Liability (CGL) insurance policy in an amount no less than $500,000, or the ability to obtain such coverage if the project is awarded.
- Bidders shall provide evidence of an active Errors & Omissions (E&O) insurance policy in an amount no less than $500,000, or the ability to obtain such coverage if the project is awarded.

Evaluation and award:

Easterseals Blake Foundation will evaluate submissions according to the criteria below, while reserving the right to accept or reject any and all proposals, to waive any minor discrepancies or technicalities in the proposal specifications, or to cancel this RFP altogether, at its sole discretion.

- Price of RFP Item 1, RFP Item 2 (45%)
- Expertise of the firm (10%)

    - References from the last (3) organizations which had any services performed.
    - References from (3) organizations which had an assessment performed that was similar in scope.
    - The report deliverable from a similar project, redacted as may be appropriate.
- Expertise of the individuals performing the assessment (45%)
    - Educational attainment
    - Professional certifications

RFP RESPONSE COVER PAGE

Firm Name: _____

E-mail Address: _____

Telephone Number: _____

Bid response 1:

- A fixed cost all-inclusive price to deliver RFP Item 1.

_____

Bid response 2:

- A fixed cost all-inclusive price to deliver both RFP Item 1 and RFP Item 2.

_____

Bid request 3:

- A fixed cost all-inclusive hourly rate, for each of the staff that will perform the assessment, should EBF choose to engage them during or following this assessment, for areas outside the scope of the RFP.
  - Bidder will honor this supplemental hourly rate for a period of (6) months following project completion.

Name _____ Rate _____

Name _____ Rate _____

Name _____ Rate _____

Name _____ Rate _____

Name _____ Rate _____

Required attachments:

1. A summary of each of the staff that will perform the assessment, together with their area of expertise, years of experience in that area of expertise, and academic and professional / technical certifications.
2. References from the last (3) organizations which had any services performed.
3. References from (3) organizations which had an assessment performed that was similar in scope.
4. The report deliverable from a similar project, redacted as may be appropriate.
5. Evidence of an active Commercial General Liability (CGL) insurance policy in an amount no less than $500,000, or the ability to obtain such coverage if the project is awarded.
6. Evidence of an active Errors & Omissions (E&O) insurance policy in an amount no less than $500,000, or the ability to obtain such coverage if the project is awarded.