HIPAA Security Assessment Request for Proposals
Questions & Answers
4/28/2017

1. How many employees that have access to PHI are included in the Risk Assessment?

   There are approximately 500 employees included.

2. Can CBH share the number and types, including operating systems, of servers, endpoints, routers, switches, firewalls, et al, that are in scope for the project?

   There are approximately 600 systems, primarily in a Windows environment.

3. Who is the executive sponsor(s) of this project at CBH?

   The Chief Operating Officer is the Executive Sponsor.

4. Is the Vulnerability Scan Internal, External, or both?

   Both.

5. Will we have access to previous Privacy and Security Risk and Vulnerability Assessments?

   No, but successful bidder will be provided with the Security Assessments Report Table (see "Exhibit A") from the previous year.

6. Will the successful bidder be required to travel to other sites, or will the on-site work all be at the CBH main facility?

   No additional travel will be required.

7. Do you have HIPAA, HITECH and Omnibus Final Rule policies in place, that have been reviewed and approved?

   Yes.

8. Have key members of the team had HIPAA compliance training?

   All staff has had HIPAA compliance training.

9. Are partner sites in scope?

   No.

10. Is privacy and breach notification out of scope for this RFP?

    Privacy and breach notification are in scope for this RFP.

11. Regarding RFP Section III.F (page 11 of the RFP): Please provide additional insight into how each of the individual selection criteria will be weighted. In particular, what percentage of the overall score is allocated to the following:

    a. Businesses owned and controlled by minorities, women, and disabled persons
    b. Philadelphia based applicants

    CBH will consider all applications based on all of the criteria presented within this RFP and choose the firm whose proposal will most likely best suit our needs.

12. Does CBH have a workforce that is predominately stationary in their office? Or is the workforce more mobile and traveling to many different locations?

    We are transitioning to a more mobile workforce, including some work-from-home and some travel to various locations, primarily within the city of Philadelphia.

13. Is there anything that is prompting this Risk Assessment (such as a breach or OCR Audit)?

    This RFP is for a routine annual risk assessment and vulnerability assessment.

14. Will CBH provide the selected consultant with a project liaison or coordinator to assist with the coordination, planning, and communications of this project?

    Yes.

15. Has CBH performed a HIPAA assessment(s) in the past? If yes:

    Yes, it is performed annually.

16. Is CBH looking for vulnerability scanning or penetration testing as part of the engagement?

    Yes.

17. Will the successful bidder be able to perform analysis of documentation off-site?

    Yes.

18. May we receive answers to all questions submitted by bidders?

    Yes, all responses to questions that CBH has chosen to answer will be posted for the benefit of all potential Applicants at http://dbhids.org/providers-seeking-information/community-behavioral-health/cbh-contracting-opportunities/.