HIPAA Risk and Vulnerability Assessment Request for Proposals
Questions & Answers
11/22/2017

1. With regard to the project Dec 27th start date - is that reasonable considering the holidays and any possible lingering contract agreement negotiations for the selected firm?

   CBH is able to negotiate the start date and completion dates based upon the timeframes of the proposal. However, an executive summary of the final deliverables must be completed prior to the end of February 2018.

2. With the inclusion of the HIPAA Privacy piece, is a 45 day project start to final report timeline feasible?

   See response to Question #1.

3. How many facilities will the consultant need to visit and are considered in-scope?

   One facility – 801 Market Street, Floors 7, 10, and 11, Philadelphia, PA 19107.

4. How many systems (applications) handle electronic protected health information?
   a. Could you name those systems and their purpose? (e.g., Epic – EMR System)
   b. Are all these systems located in a centralized location?
   c. Are any of the systems cloud-based or hosted by a third-party? If yes, which ones?
   d. Besides the cloud-based or third-party hosted systems, are any of the systems that handle ePHI and are on-premise accessible from the Internet?

   CBH systems are located in one centralized location – 801 Market Street, Philadelphia, PA 19107 and are not external-facing. Some ePHI is stored and/or processed in cloud-based systems. These include claims processing, client information system, and SFTP for data exchange with providers and other business partners.

5. Does CBH have any HIPAA-related privacy policies currently? If yes, could you please list them?

   CBH currently has a number of policies in place that relate to HIPAA Privacy and Security. CBH does not post internal policies.

6. Is it expected that the consultant will use sampling in some cases (i.e., sampling of business associate agreements)?

   CBH utilizes a standard Business Associate Agreement for all Business Associates of CBH. Awardees may use sampling of BAAs as part of their privacy assessment, as long as the proposal clearly identifies how the organization plans to complete the privacy assessment.

7. Are responses to questions from the initial RFP release still valid?

   Although the answers to questions posted in the originally released RFP (released on 4/11/17) might be valid, they are not official, as this RFP is meant to be separate and independent of that effort. Only this RFP and its answers should be considered official sources of information.