Exhibit A - TECHNICAL ASSESSMENT Part I

1. Who or what groups will provide support for the product or service once implementation begins? If vendor controlled, what services will your area need from the Broward Health provided services?

2. Does your product require any integration or import of Broward Health data for users to login, or use your product?

3. Select all the types of data that will be collected, created, received, stored, accessed, processed, transmitted, hosted or otherwise managed.

   - □ Protected Confidential Data (FIPA)
   - □ Protected Sensitive Data
   - □ Unrestricted Data
   - □ Health Records (PHI/ HIPAA)
   - □ Financial Information/ Credit Card Information (PCI)
   - □ Social Security Numbers
   - □ Other (Please Specify) ____________________

4. Please specify all record elements being collected ____

   ____

   ____

A. Subcontractors and Employees

1. Subcontractors and Employees

   a. Will you use any person who is not an employee to collect, create, receive, store, access, process, transmit, host or otherwise manage data or information for Broward Health? If so, describe. Please provide the following information about any subcontractors or hosting companies used:

Company Name	Service Provided	Type of Relationship/Contract

   b. Are employees with access to Broward Health data subject to background checks? If so, please describe the background checks performed:

   c. Are employees with access to Broward Health data required to sign an agreement requiring them to maintain as confidential and not copy or misuse information to which they have access?

   d. Describe processes to mitigate risk at the time an employee's services are terminated or suspended (e.g. remove of logical access and collection of physical assets)

e. Will the contractor work on site or remote? Will the contractor utilize a Broward Health asset or a contactor asset to gain access?

B. Hosted or SAAS Solutions

1. Infrastructure

a. Describe the technical architecture of the proposed environment and then, illustrate the flow and storage of Broward Health's data. If available, submit a network and data flow diagram.

b. What hardware will be required, is this solution compatible with virtual or physical devices, **provide a detailed listing of all specifications (see Exhibit B)**.

c. Provide a detailed listing of all **network requirements (see Exhibit B)**.

2. Data Transmission and Storage

a. Will all of Broward Health's data be transmitted and stored exclusively in the **United States**?

b. On what types of systems are the application(s)/data stored? (e.g., Oracle, SQL, etc.)

c. Will Broward Health's application(s)/data co-exist with that of other customers?

d. What is the level of separation for the application(s)/data? This answer should include information pertaining to servers/buckets/containers and any logical access controls in place.

e. Will all data elements be encrypted at all time, including in transit and at rest?

f. If encryption is used, please identify the method(s) for encryption both at rest and in transit.

g. Does your application support TLS 1.2?

h. Does your application support IPv6?

i. What do you do with data on your systems once the contract is terminated?

j. If the contract is terminated what is the process to return the data to Broward Health? What is the format?

k. What additional costs will Broward Health incur to get data returned in the event of a contract ending?

l. If custom applications are developed, please describe any security frameworks used (e.g. OWASP) or formal processes in place (e.g. Secure SDLC)

m. Do you do any data mining on Broward Health data? Or will you use Broward Health data for 3rd parties?

3. Identity and Access Management

a. Will your application require access to the Broward Health identity services?

b. Is the application hosted on the Broward Health domain or outside?

c. What authentication methods or stores do you support? For example Directory (LDAP), Active Directory.

d. Do you provide "Just in Time" provisioning or require a feed to create users within the application to associate the authenticated user in the application? What is the attribute used to link them?

e. Does your application support federated authentication?

f. Which federated model does the application support?

g. How does the product manage who is granted access to this application? For example: is it roles based from the directory or is it managed at the application tier?

4. Disaster Recovery

a. Do you have a disaster recovery plan? If so, describe.

b. Do you have a backup or redundancy/high availability process? If so, provide the configuration in detail.

c. Please identify the approved method used for data backup (e.g. Tape, VM snapshot, Amazon EBS, etc.) if hosted.

d. How/where are the backups or VM snapshots stored (stored exclusively in the United States) if hosted?

e. Are all hosted backups encrypted?

f. If hosted and you use tapes, what is the method used to transfer them from the tape storage facility to the data center?

g. If hosted how will Broward Health's data/application be protected at that recovery location(s)?

5. Service Level Agreements

a. Do you have service level agreements? If so, describe in detailed.

b. What are your maintenance cycles and how do you inform customers of future outages?

c. Do you provide availability metrics/dashboards? How do you calculate your metrics? What exceptions are granted in your metrics?

6. Audits (Internal/External) and Controls

a. Does your company complete a SSAE16 (SOC 1/2/3) Audit? If yes, when was the last one completed?

b. Does your company complete an ISO27001 or ISO27002 Audit for your application and are you ISO certified? If yes, how often and when was the last one completed?

c. Does your company complete a PCI-DSS/DA v2/v3 Audit for your application? If yes, how often and when was the last one completed?

d. Does your company complete any other third party industry audits for your application (e.g. FIPS)?

e. If your company uses a third party for auditing your application please provide the last time it was completed?

f. Do you follow information security best practices, such as those outlined in NIST 800-53 or similar standard? If so, please identify the standard used.

g. When was the last third party information security audit performed?

h. If hosted, what type of file or application auditing/logging is available?

i. Explain your ability to see what was changed, who changed it and when. Would we be able to review that information upon request?

j. What level of data access or application administration do you have?

k. Can system administrators see data or make changes to the application?

l. Do you have written information security policies that, at a minimum, govern issues such as information handling, systems hardening, user awareness training and incident response?

m. Do you have breach notification and incident reporting procedures? If so, describe.

n. Do you have a formal written incident response plan? If so, when was the last time it was tested?