Health Care District
PALM BEACH COUNTY

IT Security Vendor Questionnaire

Purpose

This document will be used by the HCDPBC to provide insight into a vendor's ability to protect the HCDPBC classified data and intellectual property.

Contact Information

Vendor Information	
Vendor Company Name:	
Point of Contact Name:	
Point of Contact Job Title:	
Phone/Contact Information:	
Signature:	
Date:	

Internal Use Only	
HCDPBC Business Owner Name:	
Line of Business:	
Phone/Contact Information:	
Signature:	
Date:	

Scoping

What type of services will you be providing to the HCDPBC?
How long have you been in business?
Has your company suffered a data loss or security breach within the last 3 years?
Are there any material claims or judgments against your organization?
Have any of your 3rd party vendors suffered a data loss or security breach within the last 3 years?

Are the answers in this questionnaire relevant to one facility or geographic location?
Are there any additional locations where scoped data and systems reside? If yes, please explain.

Business Continuity and Incident Response

Business Continuity / Disaster Recovery
Do you have a business continuity/disaster recovery plan?
How often do you test your BCP/DRP?
What is your plan for power or critical service failure?
Can the HCDPBC obtain copies of its data files upon request, in an industry standard format? (e.g. .zip, .tar, or .gz)

Backups and Failover
How long is the backup history maintained? (For example, 30 days of data on site and 60 days off-site.)
Are backups stored on-site at secured locations?
Can the database be restored to a specific day and time?
Is the failover site certified to the same standards as the primary facility? Describe.
Are the security controls for the failover site identical to those of the primary site?
Is there an active-active configuration between the primary and failover site?

Incident Response Plan
Do you have a documented Incident Response Plan?
What is your data breach handling procedure? Include notification timing, format, and contents.

Infrastructure

Do you host your product at a commercial data center, or on your own servers?
Is your data center located in the USA? If not please specify the location.
If at a data center, is it SSAE-16 (formerly SAS-70) or PCI certified?
Who maintains the server infrastructure?
Is there a hardware-based firewall that protects your data from the Internet?
What level of data center redundancy?
What is the level of Internet access redundancy?
Do you use multiple ISPs or other availability measures to guard against threats and errors?
Do you have the capacity to handle your peak load?
Please provide historical data on availability.
If the data center experiences a power outage, how many days can the generator continue to support the systems without refueling?

Physical Security

Is there a physical security program in place?
Are physical security and environmental controls in the data center and office buildings?
Are visitors permitted in the facility? If yes, describe your visitor management procedures.
Is there a sign-in procedure for all third party individuals including visitors, service providers, etc.?
Are all visitors to secure areas escorted by authorized personnel?
Do all employees and contractors wear security ID badges at all times?
Are secure areas protected by demising walls?
What kind of technology is used to control access to sensitive areas (swipe technology, biometric scanners, etc.)?
What kind of non-technology access controls are used to protect sensitive areas?
If a dedicated infrastructure is required, can you ensure it is isolated?
Are all secure areas monitored with CCTV 24 x 7 x 365?

Data and Network Security

Is it explicit in the contract that the HCDPBC's data is owned by the Health Care District of Palm Beach County?
Is data encrypted at rest?
Is data encrypted in transit? What transfer methods are used to move data? How are connections encrypted?
What is your password policy? List minimum length, complexity, expiration period, etc.
Are individuals IDs required for user authentication to applications, operating systems, databases, and network devices?
Is multi-factor authentication required to access the environment containing HCDPBC data?
Is there a process which allows you to list who from any third parties will have access to HCDPBC data?
Is there virus protection on the servers?
Does your organization use a third-party security assessment firm for penetration testing? If so, please provide a Letter of Attestation or proof of services rendered.
How promptly are security patches applied?
Are all available high/extreme-risk security patches applied and verified at least monthly?
Are systems and applications a part of this patch management process?
How is employee access to data recorded?

Vulnerability Management

Is there a documented vulnerability management program in place?
Most recent vulnerability assessment date:
Have all Extreme/High vulnerabilities been mitigated?
Please provide Letter of Attestation or copy of the most recent scan.
What is the frequency of vulnerability scanning?
Describe your vulnerability remediation process.

Identity Management

Can you integrate directly with HCDPBC directories, and what is the architecture of the integration?
How are user IDs and access credentials secured?
List steps for provisioning and de-provisioning of accounts.
If SSO is supported, to which standard?
If Federation is supported, to what standard?

Personnel Security

Do you perform background checks for:	
Criminal:	Y / N
Credit:	Y / N
Confirmation of employment:	Y / N
Confirmation of education and technical/industry credentials?	Y / N

Application Security

Do you have a documented software development lifecycle process (SDLC), and is security integrated into this process?
What are the testing and acceptance procedures for outsourced and packaged application code and third-party apps?
What application security methods (e.g. application level firewall or database auditing) are used?

Privacy

How is critical data such as credit card numbers, PHI, and ePHI masked and limited to authorized individuals?
Will data collected about the HCDPBC be shared with third parties?
What customer data is collected, how is it stored, and how long retained?
What application security methods (e.g. application level firewall or database auditing) are used?
Can you guarantee that third party access to shared logs will not reveal information critical to the HCDPBC or its personnel?
Under what conditions could third parties, including government agencies, have access to the HCDPBC's data?

Cloud Security

*Applicable only for cloud providers

Are Cloud Services provided? If yes, what service model is provided (select all that apply):	
Software as a Service (SaaS)?	Y / N
Infrastructure as a Service (IaaS)?	Y / N
Private cloud?	Y / N
Public cloud?	Y / N
Community cloud?	Y / N
Hybrid cloud?	Y / N

Is there a client management portal which allows distributed business accounts (business units/departments) to be managed under a single central corporate account?
Are application self-service features or an Internet accessible self-service portal available to clients?
Can clients run their own security services within their own cloud environment?
Is there a management approved process to ensure that image snapshots containing scoped data are authorized prior to being snapped?
Is there a formal process to ensure clients are notified prior to changes being made which may impact their service? If yes, what is the communication method?
Is there a scheduled maintenance window? If yes, what is the frequency?
Is there a scheduled maintenance window which results in client downtime? If yes, what is the downtime?
Is there an online incident response status portal, which outlines planned and unplanned outages? If yes, how long after an unplanned outage is this updated?
How are digital identities and credentials protected for use in cloud applications?

Logs and Audit Trails

Can you accommodate a timely forensic investigation?	
What access would the HCDPBC have during an investigation? How would access be provided?	
Is network traffic, and file and server access logged on the following:	
• Databases and servers	Y / N
• Active directory	Y / N
• Web and mail servers	Y / N
• Security systems (AV, UTM, IDS/IPS)	Y / N
• VPN systems	Y / N
• VM systems	Y / N
• Network switches, routers, taps, etc.	Y / N
Do logs record who accessed the system?	
Do logs record data accessed or changed?	
Are logs available to the HCDPBC upon request?	
Can the HCDPBC obtain dedicated storage for logs and audit trails? How would that access be provided?	
How long are logs and audit trails retained?	
How do you prevent tampering or alteration of logs and audit trails?	

Compliance

Are you: SAS 70 or SSAE compliant?
ISO27001 compliant?
Do you have SSAE 16 SOC2 Type 2 certification?
Please provide an Attestation of Compliance (AoC) for Payment Card Industry Data Security Standard (PCI DSS) compliance.
Can you prove compliance with HIPAA?
Can you prove compliance with the Florida Information Protection Act (FIPA)?
Can you prove compliance with the General Data Protection Regulation (GDPR)?