State of Iowa Department of Human Services

Vendor Questionnaire v3.0

March 2016

Vendor Questionnaire		
Question		(Enter Name and Date) **Response**
Data Ownership and Protection		
1	**In what geographic location(s) is DHS data stored, and how rapidly will DHS be notified if this changes?**	
2	**How does DHS get its data if the Vendor goes out of business or DHS terminates the contract?**	
3	**How does the Vendor detect changes to the integrity of DHS data and what measures are in place to ensure DHS data is not lost or destroyed?**	
4	**What happens to DHS data if the Vendor is purchased by another company?**	
5	**How is DHS data protected while it is stored? Is it encrypted? Does DHS control the encryption key?**	
6	**How does the Vendor detect and report a compromise to DHS data or services?**	
7	**What protections does the Vendor provide for protected health information ("PHI") (as the term is defined in the Health Insurance Portability and Accountability Act of 1996, ("HIPAA") regulations, and personally identifiable information ("PII") (which more generally encompasses any individually identifiable information, regardless of whether it relates to health care)?**	
8	**How does the Vendor ensure deleted data cannot be recreated?**	

9	**Will DHS data be provided to cloud service providers you utilize? How can DHS be assured cloud service providers meet the same standards for security?**	
10	**What means are provided for DHS to audit the Vendor's access to DHS data and services and the Vendor's service provider access to DHS data and services, if applicable?**	
11	**If the Vendor is currently not using a cloud environment but plans to implement in the future, will DHS be notified of the cloud environment and be provided the opportunity to review the services? If not, so state.**	
User Identity Management and Federation		
12	**How does the Vendor identify users?**	
13	**What credentials are required to access DHS data and applications (e.g. username and password)?**	
14	**What two-factor authentication mechanisms do you support?**	
Regulatory Compliance		
15	**Is the Vendor a HIPAA covered entity?**	
16	**Does any of the Vendor staff receive HIPAA training? Please explain.**	
17	**Would the Vendor be considered a business associate under HIPAA? In any circumstance, or specifically in relation to this exchange?**	
18	**Does Vendor staff receive HIPAA training? Please explain.**	
19	**Is Vendor FedRAMP Compliance Certified?**	
20	**How does the Vendor demonstrate regulatory compliance with regards to data security and privacy?**	

21	**Is the Vendor audited by third parties? What audit or security framework is used?**	
22	**What is the Vendor's information security risk assessment and management process?**	
Business Continuity and Resiliency		
23	**How does the Vendor ensure DHS can continue doing business at all times, even if there is a permanent catastrophic failure or natural or man-made disaster where DHS data or services are located?**	
24	**What standards does the Vendor follow for business continuity (e.g. ASIS/BSI BCM.01:2010)? Is the Vendor certified?**	
25	**Does the Vendor have a business continuity plan?**	
26	**How often is the business continuity plan tested?**	
27	**How are backups of DHS data protected and are off-site backups utilized? What facilities store off-site backups?**	
28	**What guarantees are provided for recovery time objectives (RTO) and recovery point objectives (RPO)?**	
User Privacy and Secondary Uses of Data		
29	**What is the Vendor's privacy policy covering information other than PHI and PII?**	
30	**Do you collect data about DHS activity and DHS employee activity in your system and use that data for purposes outside the scope of your contracted services with DHS??**	
Service and Data Integration		
31	**How does DHS access DHS data and services from the DHS office?**	
32	**How is DHS data encrypted as it flows across the network between the DHS location and the Vendor's?**	

33	**What is the Vendor's FIPS 140-2 compliancy status?**	
34	**Is data at rest on the Vendor's servers encrypted in a manner consistent with *HHS Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals?***	
35	**Is data transmitted to DHS encrypted in a manner consistent with *HHS Guidance to Render Unsecured PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals?***	
36	**How does the Vendor monitor data flowing into the Vendor's network for malware and other attacks?**	
37	**What tools and procedures does the Vendor utilize for intrusion detection and how is this capability tested for functionality at the hardware, network, and database levels.**	
Multi-Tenancy		
37	**How does the Vendor separate DHS data and services from those of other clients?**	
38	**In what ways could the Vendor's other client's affect the quality of the service or service levels provided to DHS?**	
39	**What resources will DHS be sharing with other clients?**	
40	**How does the Vendor manage the software upgrade process? What are DHS responsibilities?**	
Infrastructure and Application Security		
41	**Who owns and operates the Vendor's data centers and what physical and environment security measures are in place?**	
42	**What parts of the Vendor's infrastructure are owned and operated by the Vendor and what parts are obtained from a service provider?**	

43	**What standards are followed for hardening network equipment, operating systems, and applications?**	
44	**Who has access to the systems providing DHS data and services? How is this access controlled?**	
45	**How does the Vendor perform vulnerability and risk assessments?**	
46	**How does the Vendor use third-party penetration testing for assessing infrastructure and application security?**	
47	**When equipment is retired or replaced for repair, how does the vendor purge any resident DHS data prior to disposal.**	
48	**Explain how the vendor has implemented secure application development techniques in order to ensure security is established at the beginning of development in order to minimize known vulnerability types and eliminate website vulnerabilities identified in the latest published OWASP Top 10 list?**	
Non-production Environment Exposure		
49	**How many copies are made of DHS data and where are these copies located?**	
50	**Who has access to copies of DHS data?**	
51	**Which copies are de-identified and which are not?**	
52	**How are copies of DHS data protected?**	
53	**What capabilities are provided to DHS to audit the Vendor's access to copies of DHS data?**	