OFFICIAL RESPONSES TO VENDOR QUESTIONS
RFP # RFP-2022-DPHS-02-NEWBO

No.	Question	Answer
1.	**Section 1 Introduction, Subsection 1.2 Contract Period** Will the incumbent vendors contract term start April 1, 2022 or July 1, 2022?	The anticipated contract term is anticipated to be July 1, 2022, or upon Governor and Executive Council approval, whichever is later.
2.	**Section 3 Statement of Work, Subsection 3.1 Scope of Services.** If the selected Vendor meets the performance measure stated in Section 3.3.3, that means the selected Vendor also meets the requirement listed in section 3.1.10?	Yes.
3.	**Section 3 Statement of Work, Subsection 3.5 Compliance, Paragraph 3.5.5 Culturally and Linguistically Appropriate Services** What are the specific LEP requirements that the successful bidder must fulfill?	See Appendix C CLAS Requirements.
4.	**Appendix A - P37 Section 18, Choice of Law and Forum**	No. The selected Vendor must agree paragraph 18 of the General Provisions (Form P-37), Choice of Law and Forum.

No.	Question	Answer
	Is it acceptable to remain silent on choice of law and venue?	
5.	**Appendix A – P37, Exhibit I – Business Associate Agreement** Is it acceptable to define the timeline for this notification as within three (3) business days of the time that the Business Associate becomes aware of any use or disclosure of protected health information not provided for by the BAA?	No, the timeline for notification may not be modified to three business days. The Department has adopted a standard that requires immediate notification once the Contractor has determined there is an incident or breach, suspected or known to have placed PHI, PI or Department Confidential Data at risk of loss. The standard is part of the compliance program of the Department and is reported to our regulators.
6.	**Appendix A – P37, Exhibit I – Business Associate Agreement** Is it acceptable to define the timeline for completion of the risk assessment as within three (3) business days of the breach?	Upon notification of an incident or breach the Department will provide the Contractor with a DHHS Risk Assessment Report for Contractors. This is a summary requesting the basic information based on information available at the time. It should be returned within 24 hours or receipt by the Contractor. A final report should be provided promptly after the Contractor has completed its full investigation. There is no timeline for when the investigation should be complete, as that is matter dependent on the specific facts and the Contractor's investigation of the incident or breach
7.	**Appendix A – P37, Exhibit K – DHHS Information Security Requirements** Is it acceptable to add FedEx and UPS as acceptable transmission methods?	Yes.
8.	**Appendix A – P37, Exhibit K – DHHS Information Security Requirements**	Yes.

No.	Question	Answer
	If the selected Vendor utilizes two SFTP jobs. One is on a 24-hour cycle and is deleted the next time it is run. The other is a weekly extract. This one remains on the SFTP server for one week and is deleted once per week. Is this acceptable?	
9.	**Appendix A – P37, Exhibit K – DHHS Information Security Requirements** Is it acceptable to use the principles of NIST 800-53, as defined by that Federal Standard at a Moderate level, as the benchmark for safeguard level and scope requirements?	The Contractor is required to safeguard the Department's regulated data using the appropriate security controls and level based on federal and state laws and NIST and FIPS standards for federally regulated data based on the type(s) of Department regulated information processed, stored, and transmitted on their or a sub-contractors system(s).
10.	**Appendix A – P37, Exhibit K – DHHS Information Security Requirements** Is acceptable to define the timeline for this notification of a security breach as within three (3) business days of the time that the Contractor learns of the occurrence of a security breach?	For the Department's regulatory compliance security incident/breach notification, timing is not negotiable. Please see Department's response to Q&A item #6. However, the Department would be open to revising the Data loss language to the following: A. The Contractor must notify NHDHHS Information Security via the email address provided in this Exhibit, of any known or suspected Incidents or Breaches immediately after the Contractor has determined that the aforementioned has occurred and that Confidential Data may have been exposed or compromised. B. 1. Parties acknowledge and agree that unless notice to

No.	Question	Answer
		the contrary is provided by Department in its sole discretion to Contractor, this Section VI.1 constitutes notice by Contractor to Department of the ongoing existence and occurrence or attempts of Unsuccessful Security Incidents for which no additional notice to Department shall be required. "Unsuccessful Security Incidents" means, without limitation, pings and other broadcast attacks on Contractor's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. C. Comply with all applicable state and federal suspected or known Confidential Data loss obligations and procedures. Per the terms of this Exhibit the Contractors and End User's security incident and breach response procedures must also address how the Contractor will: 1. Identify incidents; 2. Determine if Confidential Data is involved in incidents; 3. Report suspected or confirmed incidents to the Department as required in this Exhibit. The Department will provide the Contractor with a NH DHHS Security Contractor Incident Risk Assessment Report for completion. 4. Within 24-hrs of initial notification to the Department, complete the initial NH DHHS Security Contractor Incident Risk Assessment Report and email it to the Department's Information Security Office at the email

No.	Question	Answer
		address provided herein; 5. Identify and convene a core response group to determine the risk level of incidents and determine risk-based responses to incidents and mitigation measures, prepare to include the Department in the incident response calls throughout the incident response investigation; 6. Identify incident/breach notification method and timing; 7. Within one business week of the conclusion of the Incident/Breach response investigation a final written Incident Response Report and Mitigation Plan is submitted to the Department's Information Security Office at the email address provided herein; 8. Address and report incidents and/or Breaches that implicate personal information (PI) to the Department in accordance with NH RSA 359-C:20 and this Agreement; 9. Address and report incidents and/or Breaches per the HIPAA Breach Notification Rule, and the Federal Trade Commission's Health Breach Notification Rule 16 CFR Part 318 and this Agreement. C. All legal notifications required as a result of a breach of information, or potential breach, collected pursuant to this Contract shall be coordinated with the State. The Contractor shall ensure that any subcontractors used by the Contractor shall similarly notify the State of a Breach, or potential Breach immediately upon discovery, shall make a full disclosure, including providing the State with all available information, and shall cooperate fully with the State, as defined above.

No.	Question	Answer
11.	**Appendix A – P37, Exhibit K – DHHS Information Security Requirements** Is it acceptable to add language clarifying that DHHS may conduct onsite inspections to monitor compliance with this Contract annually, upon thirty (30) days' notice?	The Department would be open to revising language to the following: The Contractor is responsible for oversight and compliance of their End Users. DHHS reserves the right to monitor compliance with this Contract, including the privacy and security requirements provided herein, HIPAA, and other applicable laws and Federal regulations until such time the Confidential Data is disposed of in accordance with this Contract.
12.	Appendix A – P37, Exhibit K – DHHS Information Security Requirements Is acceptable to define the timeline for this notification of any Security Incidents and Breaches as within three (3) business days of the time that the Contractor learns of any Security Incidents or Breaches?	No. Please see Q& A responses to item #'s 6 and 10.