OFFICIAL RESPONSES TO VENDOR QUESTIONS
RFP-2023-DPHS-05-HEALT

No.	Question	Answer
1.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section A Definitions** **a. Can the Department modify the definition of "breach?"** **b. Can the Department modify the definition of "incident?"** **c. Can the Department modify the definition of "personal information?"** **d. Can the Department modify the definition of "protected health information?"**	a. No. b. No. c. No. d. No.
2.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section 2 METHODS OF SECURE TRANSMISSION OF DATA** **Can the Department modify "Application Encryption?"**	No.
3.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section 3 RETENTION AND DISPOSITION OF**	The Department can modify this section to read: The Contractor will only retain the data and any derivative of the data for the

No.	Question	Answer
	IDENTIFIABLE RECORDS **Can the Department modify the first paragraph?**	duration of this Contract. After such time, the Contractor will have 30 days to destroy the data and any derivative in whatever form it may exist, unless, otherwise required by law or permitted under this Contract. If it is infeasible to return or destroy the Confidential Data, protections pursuant to this Information Security Requirements Exhibit survive this contract. To this end, the Contractor must:…"
4.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section 3 RETENTION AND DISPOSITION OF IDENTIFIABLE RECORDS, Subsection B. Disposition.** **Can the Department modify this section?**	The Department can modify this section to read: 1. If the Contractor will maintain any Confidential Data on its systems (or its sub-contractor systems), the Contractor will maintain a documented process for securely disposing of such data upon request or contract termination. The Contractor will also obtain written certification for any State of New Hampshire data destroyed by the Contractor or any subcontractors as a part of ongoing, emergency, and or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire Confidential Data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion and media sanitization, or otherwise physically destroying the media (for example, degaussing) as described in NIST Special Publication 800-88, Rev 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, U. S. Department of Commerce. 2. The Contractor will provide DHHS Information Security with written certification, including date and time of data destruction, asserting that data was destroyed per this Agreement. The written certification will include all details necessary to demonstrate Confidential Data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and Contractor prior to destruction. In the event where the contractor has comingled Confidential Data and the destruction is not feasible the State and Contractor will jointly evaluate regulatory and

No.	Question	Answer
		professional standards for retention requirements prior to destruction. 3. Unless otherwise specified in the Contract, within thirty (30) days of the termination of this Contract, Contractor agrees to destroy all hard copies of Confidential Data using a secure method such as shredding. 4. Unless otherwise specified in the Contract, within thirty (30) days of the termination of this Contract, Contractor agrees to completely destroy all electronic Confidential Data by means of data erasure, also known as secure data wiping.
5.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section 4 PROCEDURES FOR SECURITY, Subsections 14-16.** **Can the Department modify these sections?**	The Department may modify these sections.
6.	**Appendix A – P-37 and Standard Exhibits – Exhibit K, Section 5 Loss Reporting** **Can the Department modify this section?**	The Department can modify this section to read: 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. 1. Parties acknowledge and agree that unless notice to 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

No.	Question	Answer
		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. B. 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: 2. Identify incidents; 3. Determine if Confidential Data is involved in incidents; 4. 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. 5. 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 address provided herein; 6. 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

No.	Question	Answer
		response investigation; 7. Identify incident/breach notification method and timing; 8. 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; 9. 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; 10. 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.