OFFICIAL RESPONSES TO VENDOR QUESTIONS
RFP-2023-DMS-04-MEDIC

No.	Question	Answer
1.	**Section 3, Statement of Work, Subsection 3.1. Scope of Services, Paragraph 3.1.1** a) Does the Department anticipate that each of the three (3) MCOs plus the one (1) Dental MCO will receive an MLR audit each SFY? b) Does each MCO submit only a single MLR or are there separate MLRs for CHIP or certain populations (i.e. expansion)? c) If there are separate MLRs for each MCO, can the Department describe how many audits are needed per MCO? d) Although not part of the MLR calculation, the annual reporting requirements in 42 CFR 438.8(k) require each MCO to report their Non-claims (Administrative expenses) in addition to the MLR required components. Are the Department's expectations that the audit scope of work be inclusive of these Non-claims costs or would the audits be	a) Yes. b) At this time, MLR reporting is split by population, including Standard and Expansion populations. c) One annual SFY MLR audit is required for each MCO (3 Medicaid Health Plan MCOs; 1 Dental Managed Care MCO), including Standard and Expansion populations. d) The scope of work shall be solely to the components affecting the MLR calculation.

No.	Question	Answer
	limited solely to the components affecting the MLR calculation?	
2.	**Section 3, Statement of Work, Subsection 3.1. Scope of Services, Paragraph 3.1.7** Does the Department anticipate that the selected Vendor would conduct an audit of the encounter data in addition to the MLR?	The selected Vendor must review internal controls (e.g., protocols, procedures) for purposes of reporting, as well as MLR reports, financial reports, and encounter data, to ensure compliance with federal definitions and regulations.
3.	**Section 6. Proposal Process, Subsection 6.2, Procurement Timetable** What is the date of RFP award?	Please refer to *Section 1. Introduction, Subsection 1.2. Contract Period*, of the RFP.
4.	**Section 7. Proposal Outline and Requirements, Subsection 7.2. Outline and Detail, Paragraph 7.2.5** Can the State confirm that the only requirement for this Paragraph is to respond to the nine (9) questions in the Scope of Work and no other approach or technical details are needed?	Vendor responses to the nine (9) questions in the Scope of Work must include the Vendor's approach and any technical details, as applicable.
5.	**Section 7. Proposal Outline and Requirements, Subsection 7.2. Outline and Detail, Paragraph 7.2.6. Description of Organization; Subparagraph 7.2.6.1. Organization Summary, Part 7.2.6.1.14** In reference to the "length, depth, and	Yes.

No.	Question	Answer
	applicability of all prior experience" for the Vendor, is it acceptable to refer to our answer to RFP Question 2. Describe your experience with federal MLR calculations and auditing Medicaid MCOs?	
6.	**Appendix A – Form Number P-37 (General Provisions), Section 6 (Compliance by Contractor with Laws and Regulations/ Equal Employment Opportunity** Can the Department modify P-37 Sections 6.1 to read: 6.1 Contractor will comply with all laws, as then in effect, to the extent applicable to its Services performed pursuant to the finally negotiated Agreement.	The Department may negotiate proposed revisions to Section 6.1 with the selected Vendor.
7.	**Appendix A – Form Number P-37 (General Provisions), Section 7 (Personnel)** Can the Department modify the P-37 Section 7.2?	The Department may negotiate modifications to Section 7.2 with the selected Vendor.
8.	**Appendix A – Form Number P-37 (General Provisions), Section 8 (Event of Default / Remedies)** Can the Department modify P-37 Section	The Department may negotiate these provisions with the selected Vendor.

No.	Question	Answer
	8?	
9.	**Appendix A – Form Number P-37 (General Provisions), Section 9 (Termination)** Can the Department modify P-37 Section 9.1?	The Department may negotiate this provision with the selected Vendor.
10.	**Appendix A – Form Number P-37 (General Provisions), Section 10 (Data / Access / Confidentiality/Preservation)** Can the Department modify P-37 Section 10?	The Department may negotiate this provision with the selected Vendor. Please refer to the Information Security Requirements Exhibit for the definition of Confidential Data/Information and the non-negotiable terms and conditions regarding ownership, retention and destruction of Confidential Data/Information.
11.	**P-37 (General Provisions), Section 12 (Assignment / Delegation / Subcontracts)** Can the Department modify P-37 Section 12.3?	The Department may negotiate this provision with the selected Vendor.
12.	**Appendix A – Form Number P-37 (General Provisions), Section 13 (Indemnification)** Can the Department modify P-37 Section 13 to read below: Contractor will indemnify the State, its affiliates, officers, directors and	No, the Department cannot accept these proposed revisions to Section 13 of the General Provisions.

No.	Question	Answer
	employees against any liability incurred by the State in connection with a third party claim only to the extent directly arising out of Contractor's negligent acts or omissions or bad faith conduct in connection with Contractor's performance of its obligations under the Agreement or Contractor's material breach of its representations and warranties under the Agreement. Contractor should have no responsibility for any losses, liabilities or damages to the extent they are attributable to the acts or omissions of an indemnified person or any third party other than Contractor's subcontractors.	
13.	**Appendix A – Form Number P-37 (General Provisions), Section 14 (Insurance)** Can the Department modify P-37 Section 14?	The Department may negotiate changes to Section 14 of the P-37 with the selected Vendor; however, the amount of required coverage will not be decreased.
14.	**Appendix A – Form Number P-37 (General Provisions), Section 23 (Severability)** Can the Department modify P-37 Section 23?	The Department may negotiate modifications to this provision with the selected Vendor.

No.	Question	Answer
15.	**Appendix A – Form Number P-37 (General Provisions)** Additional Terms: Can the Department add the additional terms? a. Contractor's limitation of liability for any and all losses, liabilities or damages arising out of or relating to the provision of Services by Contractor is an amount not to exceed the greater of one times the compensation paid to Contractor for the Services giving rise to such loss. In no event should either party be liable in connection with the Agreement for loss of profits or any indirect, incidental, punitive, special or consequential damages arising in any manner from the Agreement regardless of foreseeability thereof. b. Each party and its respective affiliates will comply with our respective obligations arising from data protection and privacy laws in effect from time to time to the extent applicable to the Agreement and the Services. c. The State will provide all necessary	a. The Department may negotiate a reasonable limitation of liability with the selected Vendor. Any limitation of liability must exclude the Vendor's obligations to indemnify the Department for third party claims, data breach liability, breach of the Business Associate Agreement, and fraud or willful misconduct. b-g: The Department may negotiate modifications to this provision with the selected Vendor. **<u>*Modifications to limitation of liability are not guaranteed*</u>**

No.	Question	Answer
	and reasonably requested information, direction and cooperation to enable Contractor to provide the Services, and any direction (whether verbal or written) shall be effective if contained expressly in the applicable Statement of Work or if received (whether verbally or in writing) from a person known to Contractor or reasonably believed by Contractor to be authorized to act on the State's behalf. Contractor shall be permitted to use all information and data supplied by or on behalf of the State without having independently verified the accuracy or completeness of it. d. IN THE EVENT OF A DISPUTE BETWEEN US ARISING OUT OF OR RELATING TO THIS AGREEMENT, WE EACH AGREE TO WAIVE AND NOT DEMAND A TRIAL BY JURY. e. Survival. Any sections that by their nature or meaning should survive the termination or expiration of the Agreement should survive the termination or expiration of the Agreement. f. Advice on Legal Matters: Contractor is not engaged in the practice of law and	

No.	Question	Answer
	the Services provided hereunder, which may include commenting on legal issues or drafting documents which could constitute legal advice, do not constitute and are not a substitute, for legal advice. g. No Third Party Beneficiaries. Neither this Agreement nor the provision of the Services is intended to confer any right or benefit on any third party, other than the affiliates of each party that execute a statement of work, and, in such event, solely as set forth in such statement of work and this Agreement. The provision of Services under this Agreement cannot reasonably be relied upon by any third party.	
16.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) a** a) Will the Department change "immediately" to "promptly?" b) Will the Department add: "The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but	a) The Department cannot accept this change. b) Yes, the Department accepts this proposed additional language

No.	Question	Answer
	Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity shall be required. "Unsuccessful Security Incidents" shall include, but not be limited to, pin gs and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI."	
17.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) b** a) Will the Department change "immediately" to "promptly?" b) Can the Department change this to: The Business Associate shall complete the risk assessment within <u>three (3) business days</u> of <u>its knowledge of</u> the breach and <u>promptly</u> report the findings of the risk assessment in writing to the Covered Entity.	a) No. b) No. However, the Department agrees to amend the second paragraph after the bullets to read, "The Business Associate shall complete the risk assessment report as soon as the investigation is completed and report the findings of the risk assessment report in writing to the Covered Entity as soon as possible thereafter

No.	Question	Answer
18.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) c** Will the Department add "applicable" as follows: The Business Associate shall comply with all applicable sections of the Privacy, Security, and Breach Notification Rule.	Yes.
19.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) e** Delete: "The Covered Entity shall be considered a direct third party beneficiary of the Contractor's business associate agreements with Contractor's intended business associates, who will be receiving PHI pursuant to this Agreement, with rights of enforcement and indemnification from such business associates who shall be governed by standard Paragraph #13 of the standard contract provisions (P-37) of this Agreement for the purpose of use and disclosure of protected health information."	No. The Department agrees to revise as follows: "The Business Associate shall require all third party contractors or business associates of the Business Associate receiving PHI pursuant to the Agreement to agree to the Business Associates' rights of enforcement and indemnification from such third party or contractor who shall be governed by standards in Paragraph #13 of the standard General Provisions of (P-37) of the Agreement for the purpose of use and disclosure of protected health information. "

No.	Question	Answer
20.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) f** Will the Department change this section as follows: Within five (5) business days of receipt of a written request from Covered Entity and to the extent such release does not jeopardize the confidentiality or integrity of Business Associate's data privacy and security practices, Business Associate shall make available during normal business hours at its offices all records, books, agreements, policies and procedures relating to the use and disclosure of PHI to the Covered Entity, for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of the Agreement.	No, the Department cannot accept this change.
21.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) g** Will the Department change this section	No, the Department cannot accept this change.

No.	Question	Answer
	as follows: "or as directed by Covered Entity, to an individual"	
22.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (3) 1** Will the Department change this section as follows: "If Covered Entity, in its sole discretion, requires that the Business Associate destroy any or all PHI, the Business Associate shall certify to Covered Entity that the PHI has been destroyed." and add: "Notwithstanding these or any other data retention, destruction or return provisions elsewhere in this Agreement, Business Associate may, in accordance with legal, disaster recovery and records retention requirements, store copies of Covered Entity's data in an archival format (e.g. tape backups) or in non-archival backups on secure network drives, which may not be returned or destroyed upon request of Covered Entity. Such copies are subject to the obligations as set forth in this	No, the Department cannot accept this change.

No.	Question	Answer
	Agreement."	
23.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (6) b** Can the Department make the following mutual: Business Associate must also be able to comply?	Yes, the Department can agree with deletion of 6 b and can modify as follows: "Covered Entity and Business Associate agree to take such action as is necessary to amend the Business Associate Agreement, from time to time as is necessary for Covered Entity and/or Business Associate to comply with the changes in the requirements of HIPAA, 42 CFR Part 2 other applicable federal and state law."
24.	**Appendix A – Form Number P-37 Exhibit I, (Health Insurance Portability and Accountability Act Business Associate Agreement) Section (6) d** Make mutual. Business Associate must also be able to comply.	Yes, the Department can agree with deletion of 6 d and can modify as follows: Interpretation." The parties agree that any ambiguity in the Business Associate Agreement, and the Agreement shall be resolved to permit Covered Entity and the Business Associate to comply with HIPAA and 42 CFR Part 2."
25.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section A(1)** Will the Department revise the definition of Breach? Revise the definition of Breach as follows: 1. "Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users	No.

No.	Question	Answer
	and for an other than authorized purpose have access ~~or potential access~~ to unencrypted personally identifiable information (PII), whether physical or electronic. With regard to Protected Health Information (PHI), "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.	
26.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section A(6)** Will the Department revise the definition of Incident as follows: 6. "Incident" means an act that ~~potentially~~ violates an explicit ~~or implied~~ security policy, which includes successful attempts ~~(either failed or successful)~~ to gain unauthorized access to a system or its unencrypted PII or PHI ~~data~~, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of unencrypted PII or PHI ~~data~~; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Incidents	No.

No.	Question	Answer
	include the loss of unencrypted PII or PHI ~~data~~ through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of physical or electronic mail, all of which ~~may have the potential to~~ put the unencrypted PII or PHI ~~data~~ at risk of unauthorized access, use, disclosure, modification or destruction.	
27.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section I(A)(2)** Will the Department revise the section as follows: 2. The Contractor must not disclose any Confidential Information in response to a request for disclosure on the basis that it is required by law, in response to a subpoena, etc., without first notifying DHHS so that DHHS has an opportunity to consent or object to the disclosure, unless providing such notice is prohibited by applicable law.	No.
28.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section I(A)(3)** Will the Department revise this section	Yes.

No.	Question	Answer
	as follows: 3. If DHHS reasonably notifies the Contractor in writing that DHHS has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Contractor shall be bound by such additional restrictions and must not disclose PHI in violation of such additional restrictions and shall abide by additional security safeguards required by applicable law.	
29.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(1)** Will the Department revise this section as follows: 1. If End User is transmitting DHHS data containing PII or PHI between applications, the Contractor attests the applications have been evaluated by an expert knowledgeable in cyber security and that said application's encryption capabilities ensure secure transmission via the internet.	No.

No.	Question	Answer
30.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(2)** Will the Department revise this section as follows: 2. End User may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting DHHS data, unless encrypted using industry standards.	The Department cannot accept this change due to insider threat, however, will amend the language as follows: “Contractor may not use computer disks or portable storage devices, such as a thumb drive, as a method of transmitting Confidential Data. Encrypted thumb drives may be used as a method of transmitting Confidential Data with written exception from DHHS Information Security."
31.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(3)** Will the Department revise this section as follows: 3. Encrypted Email. End User may only employ email to transmit PII or PHI over public networks (i.e. the Internet) ~~Confidential Data~~ if email is encrypted and being sent to and being received by email addresses of persons authorized to receive such information.	No.
32.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(4)** Will the Department revise this section	No.

No.	Question	Answer
	as follows: 4. Encrypted Web Site. If End User is employing the Web to transmit PII or PHI Confidential Data, the secure socket layers (SSL) must be used and the web site must be secure. SSL encrypts PII or PHI data transmitted via a Web site.	
33.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(5)** Will the Department revise this section as follows: 5. File Hosting Services, also known as File Sharing Sites. End User may not use file hosting services, such as Dropbox or Google Cloud Storage, to transmit PII or PHI Confidential Data.	No.
34.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(7)** Will the Department revise this section as follows: 7. Laptops and PDA. If End User is employing portable devices to transmit PII or PHI Confidential Data said devices	No.

No.	Question	Answer
	must be encrypted and password-protected.	
35.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(8)** Will the Department revise this section as follows: 8. Open Wireless Networks. End User may not transmit PII or PHI Confidential Data via an open wireless network. End User must employ a virtual private network (VPN) when remotely transmitting via an open wireless network.	No.
36.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section II(10)** Will the Department revise this section as follows: 10. SSH File Transfer Protocol (SFTP), also known as Secure File Transfer Protocol. If End User is employing an SFTP to transmit PII or PHI Confidential Data, End User will structure the Folder and access privileges to prevent inappropriate disclosure of information. SFTP folders and sub-folders used for	No.

No.	Question	Answer
	transmitting PII or PHI Confidential Data will be coded for 24-hour auto-deletion cycle (i.e. PII or PHI Confidential Data will be deleted every 24 hours).	
37.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section III(A)(1)** Will the Department revise this section as follows: A. Retention 1. The Contractor agrees it will not store, transfer or process data collected in connection with the services rendered under this Contract outside of the United States without the DHHS' prior written consent. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data and Disaster Recovery locations.	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "The Contractor agrees Confidential Data will only be stored, processed, disposed of or transmitted within the boundaries of the United States and it will not outsource functions, including but not limited to IT support or administrative services, relating to the State of New Hampshire or NH DHHS offshore or outside the boundaries of the contiguous United States (including Hawaii and the District of Columbia), unless written exception is provided by DHHS Information Security. This physical location requirement shall also apply in the implementation of cloud computing, cloud service or cloud storage capabilities, and includes backup data, video conferencing and Disaster Recovery locations The Contractor agrees Confidential Data will not be stored on personal devices"
38.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section III(A)(5)** Will the Department revise this section as follows:	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "The Contractor agrees Data stored in a Cloud must be in a FedRAMP, HITECH, or government compliant cloud solution, appropriate for the type of data stored and/or processed or transmitted, and comply with all applicable statutes" and

No.	Question	Answer
	5. The Contractor agrees PI or PHI stored in a Cloud must comply with all applicable statutes and regulations regarding the privacy and security. All applicable servers and devices must have currently-supported and hardened operating systems, the latest anti-viral, anti- hacker, anti-spam, anti-spyware, and anti-malware utilities. The environment, as a whole, must have aggressive intrusion-detection and firewall protection.	regulations regarding the privacy and security, including all requirements contained within this Exhibit. All Contractor or End User controlled servers and devices must follow the hardening standards as outline in NIST 800-123 (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf). As well as current, updated, and maintained anti-malware utilities (e.g. anti-viral, anti-hacker, anti-spam, anti-spyware). The environment, as a whole, must have intrusion-detection services and intrusion protection services, as well as, firewall protection. The Contractor must hold the key to the cloud solution.
39.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section III(A)(6)** Will the Department revise this section as follows: 6. The Contractor agrees to and ensures its complete cooperation with information requests from ~~with~~ the State's Chief Information Officer regarding Contractor's processes for ~~in~~ the detection of any security vulnerability of the hosting infrastructure.	No.
40.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section III(A)**	No.

No.	Question	Answer
	Can the Department revise as follows: Insert the following new language at the end of Section III(A) (Retention): "Notwithstanding anything to the contrary in this Exhibit or the Contract, but subject to the confidentiality obligations in the Contract, Contractor may (i) retain copies of Confidential Information that is required to be retained by law or regulation, (ii) retain copies of its work product that contain Confidential Information for archival purposes or to defend Contractor's work product and (iii) in accordance with legal, disaster recovery and records retention requirements, store such copies and derivative works in an archival format (e.g. tape backups), which may not be returned or destroyed. Contractor may retain DHHS' information in paper or imaged format and it may destroy paper copies if it retains digital images thereof."	
41.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section III(B)** Can the Department revise as follows: Insert the following new language at the	No.

No.	Question	Answer
	end of Section III(B) (Disposition): "Notwithstanding anything to the contrary in this Exhibit or the Contract, but subject to the confidentiality obligations in the Contract, Contractor may (i) retain copies of Confidential Information that is required to be retained by law or regulation, (ii) retain copies of its work product that contain Confidential Information for archival purposes or to defend Contractor's work product and (iii) in accordance with legal, disaster recovery and records retention requirements, store such copies and derivative works in an archival format (e.g. tape backups), which may not be returned or destroyed. Contractor may retain DHHS' information in paper or imaged format and it may destroy paper copies if it retains digital images thereof."	
42.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(4)** Can the Department revise as follows: 4. The Contractor will ensure proper security monitoring capabilities are in place to detect ~~potential~~ security incidents ~~events~~ that can impact State of	No.

No.	Question	Answer
	NH systems and/or Department confidential information for contractor provided systems.	
43.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(6)** Can the Department revise as follows: 6. If the Contractor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the Contractor will maintain a program of an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that at a minimum <u>are consistent in all material respects with</u> ~~match~~ those for the Contractor, including B~~b~~reach notification requirements.	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "If the Contractor will be sub-contracting any core functions of the Contract supporting the services thereunder, the Contractor will ensure End User(s) will maintain an internal process or processes that defines specific security expectations, and monitoring compliance to security requirements that are equivalent with the obligations imposed on the Contractor by this Agreement."
44.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(7)** Can the Department revise as follows: 7. The Contractor will work with the Department to sign and comply with all applicable State of New Hampshire and	Yes.

No.	Question	Answer
	Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s) to the extent applicable to Contractor's services and agreed upon by the parties in advance. Agreements will be completed and signed by the Contractor and any applicable sub-contractors prior to system access being authorized.	
45.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(8)** Can the Department revise as follows: 8. If the Department determines the Contractor is a Business Associate pursuant to 45 CFR 160.103, the Contractor will execute a HIPAA Business Associate Agreement (BAA) with the Department in a form mutually agreed upon by the parties and is responsible for maintaining compliance with the agreement.	No.
46.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(9)**	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "The Contractor agrees to conduct an annual certified penetration

No.	Question	Answer
	Can the Department revise as follows: Insert the following new language to the end of Subsection (9): "Notwithstanding the foregoing, if the requested System Management Survey scope is addressed in an SSAE ISAE, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of DHHS' survey request and Contractor confirms in writing there are no known material changes in the controls audited, DHHS agrees to accept such findings in lieu of performing an audit or assessment of the controls covered by the report."	testing of databases, website, web-based portals, or systems developed, implemented, managed, or supported as a deliverable for this contract. Certification of this testing will be provided to DHHS Information Security. The objective of said Penetration Testing is to identify design and/or functionality issues in infrastructure of systems that could expose Confidential Data, as well as, computer and network equipment and systems to risks from malicious activities. Within 15 days after the annual Penetration Test has been performed, the Contractor will provide DHHS Information Security with a report of security issues that were revealed. Within 45 days of testing the Contractor will provide DHHS Information Security with a remediation plan. DHHS will decide, in consultation with the Contractor, which, if any, security issues revealed from the Penetration Test will be remediated by the Contractor."
47.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(11)** Can the Department revise as follows: 11. Data Security Breach Liability. In the event of any security breach Contractor shall make efforts to investigate the causes of the breach, promptly take measures to prevent future breach and minimize any damage or loss resulting from the	No.

No.	Question	Answer
	breach. The State shall recover from the Contractor all reasonable and legally required costs of response and recovery from the breach, including but not limited to: credit monitoring services for up to 1 year, mailing costs ~~and costs associated with website and telephone call center service~~s necessary due to the breach.	
48.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(12)** Can the Department revise as follows: 12. Contractor must, comply with all applicable statutes and regulations regarding the privacy and security of PI and PHI , and must in all other respects maintain the privacy and security of PI and PHI at a level and scope that is not less than the level and scope of requirements applicable to federal agencies, including, but not limited to, provisions of the Privacy Act of 1974 (5 U.S.C. § 552a), DHHS Privacy Act Regulations (45 C.F.R. §5b), HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164) that govern protections for individually identifiable	No.

No.	Question	Answer
	health information and as applicable under State law.	
49.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(13)** Can the Department revise as follows: 13. Contractor agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements established by the State of New Hampshire, Department of Information Technology, <u>to the extent such requirements are applicable to Contractor's services and are consistent with Contractor's own Privacy and Security Program (a summary of which can be provided upon request)</u>. Refer to Vendor Resources/Procurement at https://www.nh.gov/doit/vendor/index.htm for the Department of Information Technology policies, guidelines, standards, and procurement information relating to vendors. <u>Contractor shall be provided with advance notice of any</u>	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "Contractor must, comply with all applicable state and federal laws and policies relating to the privacy and security of Confidential Data. Contractor agrees to establish and maintain appropriate administrative, technical, physical, and organizational safeguards to protect the confidentiality of the Confidential Data and to prevent unauthorized use or access to it. The safeguards must provide a level and scope of security that is not less than the level and scope of security requirements that is set forth in the principles of NIST, including SP 800-53 (Rev.4).

No.	Question	Answer
	changes to the applicable policies, guidelines, standards, and procurement information.	
50.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(14)** Can the Department revise as follows: 14. Contractor agrees to maintain a documented breach notification and incident response process. The Contractor will notify the State's Privacy Officer and the State's Security Officer of any security breach within three (3) business days of discovery ~~immediately~~, at the email addresses provided in Section VI. This includes a confidential information B~~b~~reach, or computer security incident~~, or suspected breach~~ which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "Contractor agrees to maintain a documented breach notification and incident response process."
51.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(16)(d)** Can the Department revise as follows: d. send emails containing PII or PHI over public networks (i.e. the Internet)	No.

No.	Question	Answer
	~~Confidential Information~~ only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.	
52.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)(16)(g)** Can the Department revise as follows: g. only authorized End Users may transmit the PI or PHI ~~Confidential Data~~, including any derivative files containing PII or PHI ~~personally identifiable information~~, and in all cases involving transmission over public networks (i.e. the Internet), such data must be encrypted at all times when in transit over public networks (i.e. the Internet) or when transmitted wirelessly, at rest~~, or when~~ stored on portable devices or removable media (i.e. laptop computers, CD/DVD, USB d ives, back-up tapes) as required in section IV above.	No.
53.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section IV(A)** Can the Department add the additional language as follows:	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: "Contractor is responsible for oversight and compliance of their End Users. The Department reserves the right to monitor compliance with this Contract, including the privacy and security requirements provided herein, HIPAA, and other applicable laws and Federal

No.	Question	Answer
	"Due to the confidential and proprietary nature of Contractor's operations and to protect the integrity and security of its operations and the shared nature of systems which may be used to provide the Services under this Contract, Contractor reserves the right to reasonably limit the scope of such security inspections, and require that such inspections (a) must be preceded by advance written request of no less than 30 days prior to the anticipated start date and may occur no more than once in any twelve (12) month period, barring exigent circumstances, such as DHHS' reasonable concern of an actual breach or imminent material breach of security, in which case an inspection may be performed in response to such circumstance or concern, and at a time mutually agreed by Contractor and DHHS, (b) if to be conducted by a third party, the third party must be a mutually agreed upon security assessment specialist, where such agreement by Contractor shall not be unreasonably withheld, (c) are subject to appropriate confidentiality and non-disclosure provisions, and (d) may not disrupt Contractor's normal business or IT operations."	regulations until such time the Confidential Data is disposed of in accordance with this Contract."

No.	Question	Answer
54.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section V** Can the Department revise as follows: "The Contractor must notify the State's Privacy Officer and Security Officer of any Security Incidents and Breaches <u>within three (3) business days of discovery</u> ~~immediately~~, at the email addresses provided in Section <u>VI.</u>"	No.
55.	**Appendix A, Exhibit K, DHHS Information Security Requirements, Section V** Can the Department revise as follows: "The Contractor must further handle and report Incidents and Breaches involving PHI in accordance with the agency's documented Incident Handling and Breach Notification procedures and in accordance with 42 C.F.R. §§ 431.300 - 306. In addition to, and notwithstanding, Contractor's compliance with all applicable obligations and procedures <u>that have been agreed upon in advance by Contractor</u>, Contractor's procedures must also address how the Contractor will:	No, the Department cannot accept this revision as written. However, the Department will modify this section as follows: 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 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,

No.	Question	Answer
	1. Identify Incidents; 2. Determine the type of PII or PHI ~~if personally identifiable information is~~ involved in Incidents; 3. Report ~~suspected or~~ confirmed Incidents as required in this Exhibit or P-37; 4. Identify and convene a core response group to determine the risk level of Incidents and determine risk- based responses to Incidents; and 5. Determine whether Breach notification is required under applicable law, and, if so, identify appropriate Breach notification methods, timing, source, and contents from among different options, and if the Breach was caused by the acts or omissions of Contractor, bear reasonable costs associated with the Breach notice as well as any legally required mitigation measures.	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: 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 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;

No.	Question	Answer
		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.
56.	**Appendix D – Budget Sheet** a) Column Q of this worksheet labeled Total Cost SFYs 2023 through 2026 includes a formula that only includes the Cost for	a) Yes. Please complete the updated **Appendix D – Budget Sheet (09/09/2022)** posted to the RFP's web page at: rfp-2023-dms-04-medic. b) Annual audits are required for each MCO/Dental MCO SFY.

No.	Question	Answer
	SFY 2023, 2024 and 2025. Should this formula also include SFY 2026 for each Activity? b) How many audits should the anticipated hours and total cost reflect for each SFY?	
57.	**General Questions** a) What is the maximum budget for this project? b) Is the Department working with a current Vendor on services similar to those described in the RFP scope of work?	a) Vendors must propose their best competitive price in response to this Request for Proposals (RFP). b) No.