EXHIBIT X
CAREOREGON DATA SECURITY REQUIREMENTS

1. **CareOregon Data.** CareOregon Data is defined as all confidential and proprietary business information including but not limited to contract terms, business relationships, potential collaborations, trade secrets, payor lists, Personal Information (as defined in ORS 646A.602(12)), Protected Health Information (as defined in 45 C.F.R. § 160.103), information considered confidential and restricted under other Oregon State and Federal laws, databases, strategic and financial information and other business information, the unauthorized disclosure or use of which will be highly injurious to CareOregon and its business and its relationships in amounts not readily ascertainable

2. **Security Program**. Contractor agrees to at all times maintain a well-documented security program that conforms to generally recognized industry standards, employ the use of at least one recognized security framework for its operations, and abide by all applicable laws or regulations. The security program must at a minimum include:

   a. Oversight and management of technologies used to protect CareOregon data,
   b. Proactive identification and addressing of vulnerabilities,
   c. Periodic testing of security controls, and
   d. Detection of and response to security events.

3. **Backup and Retrieval.** Contractor shall be responsible for the commercially reasonable and prudent infrastructure and maintenance of the infrastructure to provide the herein described Work. This includes, but is not limited to database backups, application backups, OS patches and upgrades, database patches and upgrades, power supply, network security, etc.

4. **Third-Party Audits.** Contractor agrees that a SSAE 18 audit certification (SSAE 18, issued by the American Institute of Certified Public Accountants) will be conducted annually, and Contractor agrees to provide CareOregon with the current SSAE 18 SOC2 Type II audit certification upon CareOregon's request.

5. **CareOregon Audits.** At any time during the term of the Contract CareOregon may independently, at its own expense, perform an audit or review of the security of Contractor's systems used to store, transmit, or process CareOregon Data. Contractor agrees to respond to all reasonable requests for documentation in the execution of that audit, such as security program documentation, system security plans (SSP), architectural or technical diagrams, security policies and procedures, internal risk assessments, and other third-party security audits and/or assessments. CareOregon may issue findings or corrective actions to the Contractor as an outcome of the audit. Contractor agrees to review, respond, and remediate the findings in good faith. Any audit requests by CareOregon must be completed in a timely manner not exceeding 30 days from data of request.

6. **Data Security.** Contractor agrees to preserve the confidentiality, integrity, and accessibility of CareOregon Data with administrative, technical, and physical measures that conform to generally recognized industry standards and best practices. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes, and updates to operating systems and applications as provided by software vendor or open-source software support.

7. **Data Storage.** Contractor agrees that any and all CareOregon Data will be stored, processed, and maintained solely on designated target servers in accordance with "Data Location" below. CareOregon Data must be encrypted while at rest, and in accordance with "Data Encryption Standard" below. Unless agreed to in writing, at no time will CareOregon Data be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as

part of the Contractor's designated backup and recovery processes and is encrypted in accordance with "Data Encryption Standard" below.

8. **Data Location.** Unless otherwise stated in the Scope of Work and approved in advance by CareOregon, the Contractor will limit the storage and transmission of CareOregon Data to data centers and network paths physically located in the continental United States. This includes the Contractor's own data center assets and any third party or subcontracted "cloud" services used by the Contractor to provide services to CareOregon.

9. **Data Encryption Standard.** Contractor agrees to encrypt all CareOregon Data regardless of location using commercially supported encryption solutions. Contractor agrees that all designated backup and recovery processes maintains data in encrypted form, including on recovery media. The Contractor shall ensure physical storage encryption modules are consistent with FIPS 140-2 "Security Requirements for Cryptographic Modules". Encryption algorithms will meet or exceed the standards defined in NIST SP 800-57 Part 3 "Recommended Key Sizes and Algorithms" and at a minimum will be deployed with no less than a 256-bit key length for symmetric encryption and a 2048-bit key length for asymmetric encryption.

10. **Data Transmission.** Contractor agrees that any and all electronic transmission of CareOregon data unless initiated by CareOregon, shall be transmitted in an encrypted state using encryption per Data Encryption Standard above, and take place solely in accordance with "Data Re-Use" below.

11. **Data Re-Use.** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in this Contract. Data shall not be distributed, repurposed, or shared across other applications, environment, or business units of Contractor. Contractor further agrees that no CareOregon Data of any kind shall be transmitted, exchanged, or otherwise passed to other contractors or interested parties except on a case-by-case basis as specifically agreed to in writhing by CareOregon.

12. **Non-disclosure and Separation of Duties.** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of CareOregon Data to that which is absolutely necessary to perform job duties.

13. **Data Breach.** Contractor shall provide notice, either orally or in writing, to CareOregon any known, actual, or suspected compromise of the security, confidentiality, or integrity of CareOregon Data ("Data Breach"). Such notice shall be made as promptly as possible under the circumstances and without unreasonable delay of any Data Breach, but in no event more than two (2) business days after Contractor reasonably believes there has been a Data Breach. Contractor shall use commercially reasonable efforts to contain such Data Breach and provide CareOregon with a detailed report that includes: (i) the nature of the unauthorized use or disclosure, (ii) the CareOregon Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. Contractor shall provide CareOregon with all reasonably available information regarding such Data Breach and provide supplemental information as it is discovered.

    Contractor may need to communicate with outside parties regarding a Data Breach, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. Discussing Data Breaches with CareOregon should be handled on an urgent as needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law, or contained in the Contract.

    The Contractor shall (1) cooperate with CareOregon as reasonably requested by CareOregon to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the Work, if necessary.

Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by CareOregon, the Contractor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws - all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

14. **Damages.** Notwithstanding any other provision in this Contract (including any limitation of liability clauses), Contractor shall indemnify, hold harmless, and defend CareOregon from and against any and all costs (including without limitation, mailing, labor, administrative costs, vendor charges), fines, liabilities, and corrective action (including without limitation, notification costs, forensics, credit monitoring services, call center services, identity theft protection services, and crisis management/public relations services) arising out of the Data Breach.

15. **Rights to Data.** Contractor and CareOregon agree that as between them, all rights, including all intellectual property rights, in and to CareOregon Data shall remain the exclusive property of CareOregon, and Contractor has a limited, non-exclusive license to access and use CareOregon Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or rights.

16. **End of Agreement Data Handling.** Contractor agrees that upon termination of the Contract it shall erase, destroy, and render unrecoverable all CareOregon Data and certify in writing that these actions have been completed within thirty (30) days of the termination of the Contract or within seven (7) days of the request of the CareOregon Contract Administrator, whichever comes first. At a minimum a "Clear" media sanitation is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitation, SP800-88, Appendix A (csrc.nist.gov).

17. **Subcontractors.** Contractor shall require all subcontractors that have access to CareOregon Data comply with these CareOregon Data Security Requirements. Upon request by CareOregon, Contractor shall disclose to CareOregon all subcontractors or service providers that have access to CareOregon Data.

18. **Legally Required Disclosures.** If Contractor is required to disclose CareOregon Data pursuant to the order of a court or administrative body of competent jurisdiction or a government agency, Contractor shall: (i) if practicable and permitted by law, notify CareOregon prior to such disclosure, and as soon as possible after such order; (ii) cooperate with CareOregon (at CareOregon's costs and expense) in the event that CareOregon elects to legally contest, request confidential treatment, or otherwise attempt to avoid or limit such disclosure; and (iii) limit such disclosure to the extent legally permissible.

19. Contractor shall provide to CareOregon relevant contact information for a Contractor's employee who CareOregon may contact any time should any security related questions, or concerns arise.