EXHIBIT X

CAREOREGON DATA SECURITY AGREEMENT FOR TIER 1 CONTRACTORS

This Data Security Agreement ("Agreement") outlines the security measures and data protection expectations between CareOregon and Contractor concerning confidential and sensitive information. This Agreement aims to ensure the secure handling of data while maintaining legal and industry compliance.

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 and Data Security.** The Contractor shall have implemented and agrees to maintain a comprehensive security program and data protection plan that meets or exceeds industry standards and applicable laws and regulations to safeguard any and all protected health information (PHI) and other sensitive data provided by CareOregon or obtained or created on behalf of CareOregon. The security program shall include a data protection plan with administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of PHI and other sensitive data. The Contractor shall provide CareOregon with a copy of its security program and data protection plan upon request. The Contractor shall promptly notify the CareOregon as defined in the Data Breach section below in the event of any actual or suspected unauthorized access, use, disclosure, theft, loss, or destruction of PHI or other sensitive data. Contractor shall conform to generally recognized industry standards, employ at least one recognized security framework for its operations such as NIST CSF, ISO 27001, Cobit or other similar, and abide by all applicable laws or regulations.

3. **Third-Party Certifications.** Contractor agrees that a SOC2 Type II certification shall be conducted annually, and Contractor agrees to provide CareOregon with the current SOC2 Type II report and any associated bridge letters or updates upon CareOregon's request. Alternative third-party audits such as ISO 27001, or HITRUST may be considered in place of a SOC2 Type II audit. Contractor agrees to provide notice to CareOregon within 30 days should compliance with this section change during the term of contract.

4. **CareOregon Audits.** At any time during the term of the Contract, not more frequently than once a year, CareOregon may at its own expense, perform a confidential audit or review of the Contractor's compliance program and 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 date of request.

5. **Data Storage and Transmission.** Contractor agrees that any and all CareOregon Data will be stored, processed, and maintained solely on designated target servers in accordance with Section entitled "Data Location" of this Agreement. CareOregon Data must be encrypted while at rest in accordance with Section entitled "Data Encryption Standard" of this Agreement. 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 Section entitled "Data Encryption Standard." Contractor further agrees that any and all electronic transmission of CareOregon Data shall be

transmitted in an encrypted state using encryption per Section entitled "Data Encryption Standard" and take place solely in accordance with Section entitled "Data Re-Use" of this agreement.

6. **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 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.

7. **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.

8. **Data Use.** Contractor agrees to use CareOregon Data solely for the purposes specified in this Contract or accompanying Data Use Agreement, if applicable. CareOregon Data shall not be shared, distributed, or repurposed across applications, environments, business units, Subcontractors or other interested third parties of Contractor without written consent from CareOregon.

9. **Non-disclosure.** Unauthorized use or disclosure of CareOregon Data is prohibited. Contractor shall implement necessary internal controls, segregation of duties, and non-disclosure agreements to prevent unauthorized access to CareOregon Data. Contractor shall limit staff knowledge of CareOregon Data to those who require access to perform job duties.

10. **Data Breach.** Contractor shall provide notice 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 one (1) business day 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. ***Breach notification shall be reported to the following email address: securityprivacy@careoregon.org.***

    It is understood that 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 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.

11. **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.
12. **Data Ownership.** Unless defined in a separate Data Use Agreement, CareOregon retains ownership of CareOregon Data. Contractor holds a limited, non-exclusive license to access and use CareOregon Data solely for fulfilling contractual obligations. Nothing herein shall be construed to confer any license or rights.
13. **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).
14. **Subcontractors.** All subcontractors with access to CareOregon Data must comply with this Agreement. Upon request by CareOregon, Contractor shall disclose to CareOregon all subcontractors or service providers that have access to CareOregon Data. Contractor shall notify CareOregon of any changes or additions of subcontractors with access to CareOregon Data.
15. **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.
16. **Contact Person.** Contractor shall designate a responsible contact person for security-related matters who may be reached within one business day. Changes to the contact person shall be communicated to CareOregon within 15 days.