



EXHIBIT X

CAREOREGON DATA SECURITY AGREEMENT FOR TIER 2 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.

- 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.
- Security Standards.** Contractor has implemented and agrees to maintain a comprehensive security program meeting and/or exceeding industry standards and legal requirements. Contractor’s security program shall 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. Contractor shall promptly notify CareOregon of any actual or suspected data breach. The Contractor shall provide CareOregon with a copy of its security program and data protection plan upon request. Contractor shall conform to generally recognized industry standards, and abide by all applicable laws or regulations.
- Security Assessments.** To ensure the ongoing protection and security of CareOregon Data, Contractor agrees to conduct a risk and security program assessment on a yearly basis. Annual assessment shall substantially align with industry best practices and regulatory requirements. Contractor shall provide CareOregon with assessment reports and updates upon request.
- CareOregon Audits.** CareOregon reserves the right to perform, at CareOregon’s expense, annual confidential audits or reviews of Contractor’s compliance program and data systems. Contractor shall respond to audit requests, provide necessary documentation, and address audit findings within 30 days, or a mutually agreed upon schedule.
- Data Handling, Storage, and Encryption.** Contractor shall store, process, and transmit CareOregon Data solely on servers located within the United States. Data at rest shall be encrypted using commercially supported encryption solutions meeting FIPS 140-2 standards and adhere to or exceed NIST 800-57 Part 3 recommendations. Strong keys shall be used for symmetric and asymmetric encryption. Electronic transmission shall utilize encryption and adhere to agreed-upon purposes.
- 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.
- 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.
- Data Breach.** Contractor shall immediately notify CareOregon of any known, actual, or suspected data breach. Contractor shall take immediate action to contain the breach, provide a detailed report, and work to

mitigate its impact. Collaboration with CareOregon during investigations and mitigation efforts is required. ***Breach notification shall be reported to the following email address: securityprivacy@careoregon.org.***

- 9. Damages.** Contractor indemnifies and holds CareOregon harmless from costs arising from data breaches, including notification, forensic, credit monitoring, and legal expenses.
- 10. 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.
- 11. End of Agreement Data Handling.** Upon contract termination, Contractor shall securely erase, destroy, and certify in writing the destruction of CareOregon Data within 30 days unless otherwise defined in a separate Data Use Agreement. Contractor will notify CareOregon if destruction is not possible due to constraints due to HIPAA security and privacy rules, State regulation, or other legal requirement.
- 12. 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.
- 13. Legal Disclosures.** Contractor shall cooperate with CareOregon in legally required data disclosures, notifying CareOregon prior to any disclosure if practicable and legally permissible.
- 14. 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.

SAMPLE