INFORMATION SECURITY CONTROLS AGREEMENT

THIS **INFORMATION SECURITY CONTROLS AGREEMENT** (the "Agreement") is effective as of _____, 2023 (the "Effective Date"), and is made by and between **INTEGRATED HEALTH RESOURCES, LLC D/B/A BEHAVIORAL HEALTH LINK**, a Georgia limited liability company having its principal place of business at 1201 Peachtree Street NE, Suite building 400 Suite 1215, Atlanta, Georgia 30361 ("BHL"), and _____, a _____ [individual, corporation, limited liability company **etc.]** having its principal place of business at _____ ("Third Party"). In consideration of the mutual agreements herein, and for other good and valuable consideration the sufficiency and receipt of which is acknowledged, the parties agree as follows:

RECITALS

WHEREAS, the BHL is a party to a Subcontract with Carelon., or an affiliate of Carelon effective as of May 22, 2023 (the "Subcontract") under which BHL provides professional services to Carelobn in support of the prime contract between the Georgia Department of Behavioral Health and Developmental Disabilities ("GDBHDD," "Department," or "Contract Sponsor") and Carelon for an Administrative Services Organization, Prime Contract Number _____, as amended;

WHEREAS, Third Party utilizes BHL's software (app.bhlweb.com / app.behavioralhelathlink.com) and accesses Carelon Confidential Information

WHEREAS, as an Carelon subcontractor, BHL is required to comply with the Carelon Required Information Security Controls Exhibit attached hereto as Exhibit A (the "RISC Exhibit"); and

WHEREAS, in addition to Third Party's obligations under its Business Associate Agreement (the "BHL BAA") with BHL a Business Associate of BHL, BHL requires Third Party to agree to comply with the RISC Exhibit in connection with the performance of services for BHL in support of the Subcontract.

NOW, THEREFORE, in consideration of the foregoing and of other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Incident Response Program. Third Party shall maintain an Incident Response Program that includes processes and procedures in place so that information security Events will be reported through appropriate communications channels as quickly as possible. As used herein "Incident(s)" means an occurrence that jeopardizes or is reasonably suspected to jeopardize the confidentiality, integrity, or availability of an - information system that stores, processes, accesses, or otherwise handles Carelon Confidential Information or the Carelon Confidential Information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies, and "Event(s)" means any observable occurrence in a system and/or network that indicates or is reasonably suspected to indicate that an incident is occurring or has occurred. Such processes

and procedures for Event reports must be tested, reviewed and updated, by Third Party periodically. All employees, contractors and third-party users of Third Party shall be made aware of their responsibility to report any information security Events prior to being granted access to any Carelon Health Confidential Information. If at any time during the Agreement, Third Party becomes aware of an ongoing information security Incident, Third party will promptly, and in no event later than 24 hours, notify BHL of the security Incident at securityresponse@ihrcorp.com. For purposes of this Exhibit, Carelon Confidential Information or Confidential Information means any data that is subject to applicable state and federal data security and privacy laws, regulations and guidance, including Carelon Health's- personally identifiable information and protected health information and any data that contains Carelon trade secrets, proprietary, competitive or sensitive information or systems information that could negatively impact Elevance Health if made public.

2. Limited Access to Carelon Confidential Information. Third Party agrees that only those individuals providing services to Elevance Health in support of the Subcontract on Third Party's behalf, or those who are responsible for administering or managing systems that contain Elevance Health Confidential Information, shall be authorized to access systems containing Elevance Health Confidential Information. Third Party further agrees that physical and logical access will be granted to the minimum Elevance Health Confidential Information necessary to meet the requirements of the user's scope of responsibilities.

3. Security Awareness Training. Third Party Security agrees to complete security awareness training prior to access being granted to Carelon Confidential Information, and then completed on an annual basis going forward so long as access to Carelon Confidential Information continues. This training should include, at a minimum, guidance on defending against malware, protecting passwords, monitoring and reporting system notifications, social engineering, and handling sensitive data.

4. Background Checks. Prior to gaining access to Carelon Confidential Information, Third Party agrees that Third Party workforce members will have appropriate background checks completed in compliance with state and federal law.

5. Obligation to Disable Access. Third Party agrees to promptly disable access for all users that are no longer required or authorized to access Carelon Confidential Information or systems that contain Carelon Confidential Information must have access by contacting securityresponse@ihrcorp.com.

6. Compromised Passwords. Third Party agrees that if a password is suspected to have been compromised, Third party agree to ensure that the password must is immediately changed or reset.

7. Access Outside US. Third Party agrees to use a Clean Room whenever regulated data such as Protected Health Information, Personally Identifiable Information, or cardholder

data as defined by Payment Card Industry-Data Security DSS is accessed from outside the United States.

8. No Offshore Wireless Access. Third Party acknowledges and agrees that Wireless access is prohibited from being used to access Carelon Confidential Information from offshore locations and will ensure that its workforce complies with this restriction.

9. Indemnity. Each party agrees to be responsible for the acts and /or omissions of its own agents and employees' performed within the scope of employment. [CSB NAME], a statutorily created public corporation of the State of Georgia, cannot waive immunity conferred by the Georgia Constitution. [CSB NAME] maintains insurance coverage through the State's risk management plan applicable to the negligent acts and omissions of its officers and employees, which occur within the scope of their employment by [CSB NAME]. [CSB NAME] has no coverage applicable to third-party acts or omissions and can undertake no obligation that might create a debt on the state treasury.

10. General. This Agreement shall be governed by, and construed in accordance with, the laws of the State of Georgia, without regard to the conflict of laws provisions thereof. The parties consent and agree that all legal proceedings relating to the subject matter of this Agreement and all disputes arising from this Agreement shall be maintained in state and federal courts sitting within the State of Georgia, and the parties consent and agree that jurisdiction for such proceedings and disputes shall lie exclusively with such courts and the venue shall be in Atlanta, Georgia.

IN WITNESS WHEREOF, each of the parties hereto has caused this Agreement to be duly executed by a duly authorized representative of such party as of the Effective Date.

Integrated Health Resources d/b/a Behavioral Health Link	**[Third Party]**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____