

AGREEMENT

Between

THE STATE OF RHODE ISLAND

**DEPARTMENT OF BEHAVIORAL HEALTHCARE,
DEVELOPMENTAL DISABILITIES & HOSPITALS**

And

VENDOR NAME

Services Provided: **Service Description**

Contract Award: **\$amount**

Procurement Method: **procurement type**

Performance Period: **Contract Term**

ADDENDA

The parties agree that the State's General Conditions of Purchase (220-RICR-30-00-13 available at <https://rules.sos.ri.gov/regulations/part/220-30-00-13>) and the addenda in this document establish the agreement between the parties. The addenda found in this agreement are as follows:

ADDENDUM E-BUSINESS ASSOCIATE AGREEMENT

ADDENDUM F-SPECIAL TERMS AND CONDITIONS

EXHIBITS

EXHIBIT A-SCOPE OF WORK

EXHIBIT B-BUDGET AND NARRATIVE

EXHIBIT C-PAYMENT AND REPORT

SCHEDULE EXHIBIT D- OIG-HHS

EXCLUSION LIST

EXHIBIT E-FALSE CLAIMS ACT ACKNOWLEDGEMENT

EXHIBIT F-WHISTLEBLOWER PROTECTION ACT ACKNOWLEDGEMENT

ADDENDUM E
BUSINESS ASSOCIATE AGREEMENT

Except as otherwise provided in this Business Associate Agreement Addendum, **Insert Vendor Name** (hereinafter referred to as the "Business Associate") may use, access or disclose Protected Health Information (PHI), to perform functions, activities or services for or on behalf of **The State of Rhode Island, Department of Behavioral Healthcare, Developmental Disabilities & Hospitals** (hereinafter referred to as the "Covered Entity"), as specified herein and the attached Agreement between the Business Associate and the Covered Entity (hereinafter referred to as "the Agreement"), which this Addendum supplements and is made part of, provided such use, access, or disclosure does not violate the Health Insurance Portability and Accountability Act (HIPAA), 42 USC 1320d et seq., and its implementing regulations including, but not limited to, 45 CFR, parrs 160, 162, and 164, hereinafter referred to as the Privacy and Security Rules and patient confidentiality regulations, and requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111-5 (HITECH Act) and any regulations adopted or to be adopted pursuant to the HITECH Act that relate to the obligations of Business Associates, Rhode Island Mental Health Law, RI General Laws Chapter 40.1-5-26, Confidentiality of Health Care Communications and Information Act, RI General Laws Chapter 5-37.3-1 et seq., Confidentiality of Substance Use Disorder (SUD) Patient Records ("2022 Part 2 NPRM"), Support Reproductive Health Care Privacy ("2023 Privacy Rule NPRM") Rhode Island Reproductive Privacy Act, RI General Law Chapter § 23-4.13-2 et seq. and Business Associate recognizes and agrees it is obligated by law to meet the applicable provisions of the HITECH Act.

1. Definitions:

2. Generally:

In this Agreement, terms used but not otherwise defined shall have the same meaning as those terms in 45 CFR §§ 160.103, 164.103, and 164.304, 164.501, and 164.502.

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA, the Privacy and Security Rules, and the HITECH Act: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, and Protected Health Information as required by Law, Secretary of Health and Human Services, Security Incident, Subcontractor, Unsecured Protected Health Information and Use

Specific:

- A. "Addendum" means this Business Associate Agreement Addendum.
- B. "Agreement" means the contractual Agreement by and between the State of Rhode Island, Department of Behavioral Health, Developmental Disabilities, and Hospitals and Business Associate, awarded pursuant to the State of Rhode Island's Purchasing Law (Chapter 37-2 of the Rhode Island General Laws) and Rhode Island Department of Administration, Division of Purchases, Purchasing Rules, Regulations and General Conditions of Purchasing.
- C. "Business Associate" generally has the same meaning as the term "business associate" at 45CFR 160.103 and, in reference to the party to this Agreement, shall mean **Insert Vendor Name**
- D. "Client/Patient" means Covered Entity funded person who is a recipient and the client or

patient of the Business Associate.

- E. "Covered Entity" generally has the same meaning as "covered entity" at 45CFR 160.103. In reference to the party to this Agreement shall mean, The State of Rhode Island, Department of Behavioral Healthcare, Developmental Disabilities, and Hospitals.
- F. "Electronic Health Record" means an electronic record of health-related information on an individual created, gathered, managed, or consulted by authorized health care clinicians and staff.
- G. "Electronic Protected Health Information" or "Electronic PHI" means PHI transmitted by or maintained in electronic media as defined in the HIPAA Security Regulations.
- H. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
- I. "HIPAA Privacy Rule" means the regulations promulgated under HIPAA by The United States Department of Health and Human Services to protect the privacy of Protected Health Information, including the Privacy, Security, Breach Notification, and Enforcement Rules 45CFR Part 160 and Part 164.
- J. "HITECH Act" means the Privacy, Security, and Security Breach Notification provisions applicable to Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, and any regulations promulgated thereunder and as amended from time to time.
- K. "Reproductive health care" means health care, as defined in this section, that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care.
- L. "Secretary" means Secretary of the U.S. Department of Health and Human Services (DHS)
- M. "Secured PHI" means PHI that was rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technologies or methodologies specified under, or pursuant to, Section 13402 (h)(2) of the HITECH Act under ARRA.
- N. "Security Incident" means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information.
- O. "Security Rule" means the Standards for the security of Electronic Protected Health Information found at 45CFR Parts 160 and 162 and Part 164, Subparts A and C. The application of Security Provisions, Sections 164.308, 164.310, 164.312, and 164.316 of Title 45, Code of Federal Regulations, shall apply to the Business Associate of Covered Entity in the same manner that such sections apply to the Covered Entity.
- P. "Suspected Breach" is a suspected acquisition, access, use, or disclosure of Protected Health Information (PHI), in violation of HIPAA Privacy Rules, as referenced above, that compromises the security or privacy of PHI.
- Q. "Unsecured PHI" means PHI that is not secured, as defined in this Section, through the use of a technology or methodology specified by The Secretary of the U.S. Department of Health and Human Services.

2. Obligations and Activities of Business Associate

- a. The Business Associate agrees not to use or further disclose PHI other than as permitted or required by this Agreement or as required by law, provided such use or disclosure would also

be permissible by law by the Covered Entity.

- b. The Business Associate shall not disclose or respond to any request or demand for PHI that is actually or potentially related to reproductive health care where the request or demand is for the purpose of health oversight activities, law enforcement activities, judicial or administrative proceedings, or disclosures to coroners and medical examiners. Business Associate agrees that it will not use, disclose, transmit, or otherwise provide PHI for the purpose(s) of a) identifying an individual, conducting a criminal, civil or administrative investigation about an individual, or imposing criminal, civil or administrative liability upon an individual, for the mere act of seeking, obtaining, providing, or facilitating lawful reproductive health care services.
The Business Associate will require that any request or demand for PHI under section B above be accompanied by a signed and valid attestation ensuring that the PHI sought is not for a prohibited purpose. Any request or demand for such PHI must be forwarded to the Department for review, together with the signed attestation from the requesting party on the attestation form provided by the Department or substantially similar to it and acceptable to the Department.
- c. The Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement. The Business Associate agrees to implement Administrative Safeguards, Physical Safeguards, and Technical Safeguards ("Safeguards") that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI as required by the "Security Rule."
- d. The Business Associate agrees to mitigate, to the extent practicable, any harmful effect known to the Business Associate of a use or disclosure of PHI by the Business Associate in violation of the requirements of the Agreement.
- e. The Business Associate agrees to report to the Covered Entity any use or disclosure of the PHI not provided for by this Agreement, including breaches of unsecured PHI as required by 45 CFR § 164.410 and any Security Incident of which it becomes aware, within twenty-four (24) hours of the Incident.
- f. The Business Associate agrees to ensure that any agent, including a subcontractor or vendor, to whom it provides PHI received from, created, or received by the Business Associate on behalf of the Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate concerning such information through a contractual arrangement that complies with 45 CFR § 164.314.
- g. The Business Associate agrees to provide paper or electronic access, at the request of the Covered Entity and in the time and manner designated by the Covered Entity, to PHI in a Designated Record Set to the Covered Entity or, as directed by the Covered Entity, to an individual to meet the requirements under 45CFR § 164.524. If the individual requests an electronic copy of the information, the Business Associate must provide the Covered Entity with the information requested in the electronic form and format requested by the individual or the Covered Entity if it is readily producible in such form and structure; or, if not, in a readable electronic form and format as requested by the Covered Entity.
- h. The Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or accepts, according to 45 CFR § 164.526 at the Covered Entity's request or an Individual, and in the manner designated by the Covered Entity. If the Business Associate receives a request for an amendment to PHI directly from an Individual, the Business Associate shall notify the Covered Entity upon receipt of such request.
- i. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by the Business Associate on behalf of the Covered Entity available to the Covered Entity, or at the request of the Covered

Entity to the Secretary of Health and Human Services, in a time and manner designated by the Covered Entity or the Secretary, for the intent of the Secretary to determine compliance with the Privacy Rule and Security Rule.

- j. The Business Associate agrees to document such disclosures of PHI and records related to such disclosures as required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI per 45 CFR § 164.528.
- k. Business Associate agrees to provide to the Covered Entity or an Individual, in a time and manner designated by the Covered Entity, information collected under this Agreement to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures for PHI per 45 CFR § 164.528.
- l. If the Business Associate accesses, maintains, retains, modifies, records, stores, destroys, holds, uses, or discloses unsecured Protected Health Information (as defined in 45 CFR § 164.402) for the Covered Entity, following the discovery of a breach of such information, the Business Associate shall notify the Covered Entity of such breach within twenty-four (24) hours after the discovery of a breach. Such notice shall include: a) the identification of each individual whose Unsecured Protected Health Information has been or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such breach; b) a brief description of what happened, including the date of the breach and discovery of the breach; c) a description of the type of Unsecured PHI that was involved in the breach; d) a description of the investigation into the breach, mitigation of harm to the individual and protection against further breaches; e) the results of any investigation performed by Business Associate related to the breach, and f) contact information of the most knowledgeable individual for Covered Entity to contact relating to the breach and its investigation into the breach.
- m. To the extent the Business Associate is carrying out an obligation of the Covered Entity's under the Privacy Rule, the Business Associate must comply with the Privacy Rule requirements that apply to the Covered Entity in the performance of such obligation.
- n. Business Associate agrees that it will not receive remuneration directly or indirectly in exchange for PHI without authorization unless an exception under 45 CFR § 164.502(a)(5)(ii)(B)(2) applies.
- o. Business Associate agrees that it will not receive remuneration for certain communications that fall within the exceptions to the definition of Marketing under 45 CFR § 164.501 unless permitted by 45 CFR § 164.508(a)(3)(A)-(B).
- p. The Business Associate agrees that it will not use or disclose genetic information for underwriting purposes, as defined in 45 CFR § 164.502.
- q. Business Associate hereby agrees to comply with state laws and rules and regulations applicable to PHI and personal information of individuals it receives from Covered Entity during the term of the Agreement.
 - i. Business Associate agrees to (a) implement and maintain appropriate physical, technical, and administrative security measures for the protection of personal information as required by any state law and rules and regulations; including, but not limited to: (i) encrypting all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly; (ii) prohibiting the transfer of personal information to any portable device unless such transfer is approved in advance; and (iii) encrypting any personal information being transferred to a portable device and (b) implement and maintain a Written Information Security Program as required by any state law as applicable.
 - ii. The safeguards outlined in the Agreement shall apply equally to PHI,

confidential, and "personal information." Personal information means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

3. Permitted Uses and Disclosures by Business Associate

- a. Except as otherwise limited to this Agreement, the Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, the Covered Entity. As specified in the Service Arrangement, such use or disclosure would not violate the Privacy Rule if done by the Covered Entity or the minimum necessary policies and procedures required by 45 CFR § 164.514(d).
- b. Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of the Business Associate or carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited to this Agreement, the Business Associate may disclose PHI for the proper management and administration of the Business Associate, under the provision that the law requires disclosures. The Business Associate requires reasonable assurances from the recipient of disclosed information that the information remains confidential and will only be used or further disclosed if required by law. The recipient will notify the Business Associate of any instances of which it is aware that the confidentiality of the information has been breached.
- d. Except as otherwise limited in this Agreement, the Business Associate may use PHI to provide Data Aggregation Services to the Covered Entity as permitted by CFR § 164.504 (e)(2)(i)(B).
- e. The Business Associate may use PHI to report law violations to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

4. Obligations of Covered Entity

- a. The Covered Entity shall notify the Business Associate of any limitation(s) in the Covered Entity's privacy practices per 45CFR § 164.520, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- b. The Covered Entity shall notify the Business Associate of any changes in, or revocation of, an Individual's permission to use or disclose PHI to the extent that such changes may affect the Business Associate's use or disclosure of PHI.
- c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to per 45 CFR § 164.522, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

5. Permissible Requests by Covered Entity

The Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by the Covered Entity, provided that, to the extent permitted by the Service Arrangement, the Business Associate may use or disclose PHI for the Business Associate's Data Aggregation activities or proper management and administrative activities.

6. Term and Termination

- a. The term of this Agreement shall begin as of the effective date of the Service Arrangement, governed by the issuance of any applicable, valid Purchase Order. The termination of this Agreement will take effect when all PHI provided by the Covered Entity or PHI created or received by the Business Associate on behalf of the Covered Entity is destroyed or returned to the Covered Entity. If it is infeasible to return or destroy PHI, protections will extend to such information according to the termination provisions of this Section.
- b. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
 - i. Provide an opportunity for the Business Associate to correct the breach or violation within a specified time provided by the Covered Entity. If the Business Associate does not rectify the breach or violation within this time, the Covered Entity will terminate this Agreement and the Service Arrangement.
 - ii. Immediately terminate this Agreement and the Service Agreement if the Business Associate has breached a material term of this Agreement and a resolution is not possible.
- c. Except as provided in paragraph (d) of this Section (6), upon any termination or expiration of this Agreement, the Business Associate shall return or destroy all PHI received from the Covered Entity or created or received by the Business Associate on behalf of the Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of the Business Associate. The Business Associate shall not retain copies of the PHI. The Business Associate shall ensure that its subcontractors or vendors return or destroy any of the Covered Entity's PHI received from the Business Associate.
- d. If the Business Associate determines that returning or destroying PHI is not feasible, the Business Associate shall provide notification of the conditions preventing the return or destruction of PHI to the Covered Entity. Upon written agreement by the Covered Entity that the return or destruction of PHI is not possible, the Business Associate will extend the protections of this Agreement to limit further use or disclosure of such PHI to those purposes that make the return or destruction not possible for as long as the Business Associate maintains such PHI.

7. Miscellaneous

1. A reference to a section of the Privacy Rule or Security Rule in this Agreement means this Section is in effect or as amended.
2. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is required for the Covered Entity to comply with HIPAA requirements, The Privacy and Security Rules, and HITECH.
3. The respective rights and obligations of the Business Associate under Section 6 (c) and (d) of this Agreement shall survive the termination of this Agreement.
4. Any ambiguity in this Agreement shall be resolved to permit the Covered Entity to comply

with HIPAA and HITECH.

5. The Business Associate is solely responsible for all decisions made by the Business Associate regarding the safeguarding of PHI.
6. Nothing expressed or implied in this Agreement intends to confer, nor shall anything herein confer upon anyone other than the Covered Entity, the Business Associate, and their respective successors and assigns any rights, remedies, obligations, or liabilities whatsoever.
7. Modifying the terms of this Agreement shall not be valid or binding upon the parties unless and until such modification is committed in writing and executed by the parties hereto.
8. This Agreement shall be binding upon the parties hereto and their respective legal representatives, trustees, receivers, successors, and permitted assigns.
9. Should any provision of this Agreement be found unenforceable, it shall be deemed severable. The balance of the Agreement shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.
10. This Agreement and the rights and obligations of the parties hereunder shall be governed by, and construed under, the State of Rhode Island laws, including all matters of construction, validity, and performance.
11. All notices and communications required or permitted to be given hereunder shall be sent by certified or regular mail. Communications to the party shall be sent to its respective address as stated in PAR.15 (Notices) of Addendum F of this Agreement or at another address as such party shall, from time to time, designate in writing to the other party and shall be effective from the date of mailing.
12. This Agreement, including such portions incorporated by reference herein, constitutes the entire Agreement by, between, and among the parties. Such parties acknowledge by their signature hereto that they do not rely upon any representations or undertakings by any person or party, past or future, not expressly set forth in writing herein.
13. The Business Associate shall maintain or cause sufficient insurance coverage as shall be necessary to the Business Associate and its employees, agents, representatives, or subcontractors against any claims or damages arising under this Business Associate Agreement. According to this Business Associate Agreement, such insurance coverage shall apply to all services provided by the Business Associate or its agents or subcontractors. The Business Associate shall indemnify, hold harmless and defend the Covered Entity from and against any claims, losses, liabilities, costs, and other expenses (including, but not limited to, reasonable attorneys' fees and expenses, administrative penalties and fines, costs expended to notify individuals and to prevent or remedy possible identity theft, financial harm, reputational harm, or any other claims or liability related to a breach) incurred as a result of, or arising out of, or in connection with, any negligent or intentional acts or omissions of the Business Associate, its employees, agents, representatives, or subcontractors, under this Business Associate Agreement. This provision shall survive termination of this Agreement.

(signatures on following page)

8. Acknowledgement

The undersigned affirms that they are a duly noted authorized representative of the Business Associate for which they are signing and have the authority to execute this Addendum on behalf of the Business Associate.

Acknowledged and agreed to by:

Vendor Name

**State of Rhode Island, Department of
Behavioral Healthcare, Developmental
Disabilities, & Hospitals**

Director

Title of Authorized Agent

Title of Authorized Agent

Printed Name of Authorized Agent

Richard Leclerc

Printed Name of Authorized Agent

Signature of Authorized Agent

Signature of Authorized Agent

Date

Date

ADDENDUM F
SUPPLEMENTAL TERMS AND CONDITIONS

This Addendum to the State's General Conditions of Purchase (220-RICR-30-00-13, available at: <https://rules.sos.ri.gov/regulations/part/220-30-00-13>) supplements and serves as additional terms and conditions to the General Conditions of Purchase ("General Conditions"). The General Conditions and items incorporated by reference in 220-RICR-30-00-13.34, including this Addendum, serve as the "Agreement" between the parties. Under the General Conditions of Purchase, 220-RICR-30-00-13.34, this Agreement serves as General Conditions Addendum F. The Contractor further agrees as follows:

WHEREAS this contract is executed between **The State of Rhode Island, Department of Behavioral Healthcare, Developmental Disabilities, & Hospitals** (hereinafter referred to as "BHDDH") or (the "State") and Vendor Name (hereinafter referred to as the "Contractor" (collectively the "Parties") for services rendered to the State as to Service Provided

WHEREAS the Contractor will perform all duties and responsibilities included in the Scope of Work as described in **Exhibit A** and adhere to the agreed-upon Budget described in **Exhibit B**.

THEREFORE, the Parties to the Agreement, for good and valuable consideration, the receipt of which is hereby acknowledged, agree as follows:

PAR 1. GOVERNING LAW AND GENERAL TERMS AND CONDITIONS

The State's Purchasing Law (Chapter 37-2 of the Rhode Island General Laws), and the Rhode Island Department of Administration, Division of Purchases, Purchasing Rules, Regulations, and General Conditions of Purchase, apply as the governing terms and conditions of this Agreement can be obtained at: <https://rules.sos.ri.gov/regulations/part/220-30-00-13>. In addition, the provisions of Federal Laws, Regulations, and Procedures governing the implementation of federal funds apply to this Agreement.

PAR 2. PERFORMANCE

In addition to obligations stated in 220-RICR-30-00-13.22, the Contractor shall perform all obligations, duties, and work under this Agreement's interim period. Said duties and responsibilities in the Scope of Work are outlined in **Exhibit A**, the Budget in **Exhibit B**, and the Payments and Reports Schedule in **Exhibit C**. **The Department of Behavioral Healthcare, Developmental Disabilities, & Hospitals** (BHDDH) shall have the right, at all times, to review the work performed, and, to that end, BHDDH shall be allowed reasonable access to all activities related to this Agreement.

PAR 3. TIME OF PERFORMANCE

The Contractor will perform under this Agreement for an initial **one-year term** commencing on Start Date

PAR 4. INDEPENDENT CONTRACTOR

The Contractor shall engage as an independent contractor of the State. Nothing contained in this Agreement will be construed to create the relationship of employer and employee, principal and

agent, partnership or joint venture, or any other fiduciary relationship. The Contractor may not act as an agent for, or on behalf of, the State or bind the State in any manner. The State shall issue an IRS Form 1099 reflecting the Contractor's compensation. The State will not be responsible for federal, state, and local taxes derived from the Contractor's net income or for the withholding or payment of any federal, state, and local income and other payroll taxes, workers compensation, disability benefits, or other legal requirements applicable to the Contractor. The Contractor will not be entitled to Worker's Compensation, Retirement, Insurance, or other benefits afforded to employees of the State.

PAR 5. PROJECT OFFICER-BHDDH

BHDDH shall appoint a Contract Manager to manage this Agreement. The Contractor agrees to maintain close and continuous communication with the Contract Manager throughout the performance of work and services undertaken under the terms of this Agreement. The Contract Manager is responsible for seeking authorization for all payments made by BHDDH to the Contractor under this Agreement. No work shall commence on the Contractor's part without a valid Purchase Order issued by The Department of Administration, Division of Purchases.

PAR 6. CONTRACTOR

The Contractor shall be responsible for coordinating and reporting work performed according to this Agreement, subject to and under the Scope of Work in Exhibit A; within the Budget in Exhibit B; and payment schedule in Exhibit C. The Contractor shall notify BHDDH in writing immediately and seek approval from BHDDH should a change to this Agreement be necessary in the Contractor's opinion. Under no circumstances will a change be undertaken without the prior written consent of BHDDH.

PAR 7. WORK REVIEWS

The Contractor recognizes the responsibilities of BHDDH to provide financial oversight of its contractors and consultants. The Contractor agrees that the scope of work performed under this Agreement may be reviewed by BHDDH, its designee, or any third party designated by BHDDH. BHDDH reserves the right to verify hours, costs, and expenses and ensure that they comply with state and federal laws, regulations, and policies or for any other reason at the sole discretion of BHDDH.

PAR 8. RESPONSIBILITIES UPON TERMINATION OR DEFAULT OF AGREEMENT

Upon termination or default of this Agreement, per 220-RICR-30-00.13.20, the Contractor will receive notice of termination specifying the nature and extent to which work performed under this Agreement is terminated. On the date upon which this termination becomes effective, the Contractor shall:

1. Stop work under this Agreement on the date and to the extent specified in the notice of termination.
2. Take such action as is necessary or as the (BHDDH) Director may reasonably instruct for the protection and preservation of property in possession of the Contractor and in which the State has or may acquire an interest related to this Agreement.
3. Terminate all orders to the extent related to the performance of work terminated in the notice.
4. Subject to provisions of this paragraph, the Contractor shall assign to the State all rights,

titles, and interests under the order of termination. The State shall have the right to settle or pay any claims arising out of the termination at its discretion. Notwithstanding this provision, the Contractor is not obligated to assign any rights, title, or interest in the absence of payment, therefore, by the State.

5. With the approval or ratification of the State, initiate settlement of all outstanding liabilities and claims arising from such termination. The cost of which would be reimbursable in whole or in part, per the provisions of this Agreement. The State shall not unreasonably withhold final approval.
6. Subject to provisions of this paragraph (8), the Contractor shall transfer title or, if the Contractor does not have the title, transfer their rights to the State (to the extent that the title has not already been transferred). The Contractor will deliver all files, processing systems, data manuals, or other documentation related to the work completed or in progress before notice of termination, in a manner and at a reasonable time as directed by the State.
7. If instructed, the Contractor will complete the performance of work not included in the notice of termination. The Contractor shall proceed immediately with the performance of the above obligations, notwithstanding any delay in determining or adjusting the amount of any reimbursable price under this clause.
8. Upon termination, the Contractor agrees to an orderly transition in accordance with 220-RICR-30- 00-13.30. Prior to the end of the termination and up to sixty (60) days thereafter, the Contractor agrees to make an orderly transition of contract and deliverables hereunder and to perform all tasks in good faith that are necessary to preserve the integrity of the work performed by the Contractor on behalf of the State. Upon termination or expiration of the Agreement, the Contractor shall, if requested by the State, at least thirty (30) days prior to such termination or expiration, provide reasonable training for the successor entity and continued performance of services. For providing such training or continued performance after the Term of the Agreement, the State shall pay the Contractor at mutually agreed rates for personnel providing such training and services, unless services delivered are defined herein and rates established, then such rates shall apply for such period. Should any missing data, materials, documents, etc., be discovered after expiration or termination, a grace period of one hundred twenty (120) days shall be in effect during which the data, materials, documents, etc., is to be provided at a predetermined cost or at no additional cost if the Contractor caused the loss. Lost data shall be provided to the State in a form acceptable to the State.

PAR. 9. ACCESSIBILITY AND RETENTION OF RECORDS

The Contractor agrees to maintain and make accessible all fiscal and activities records relating to this Agreement to the State, Federal Officials, or their designated representatives, necessary to verify the accuracy of the Contractor's invoices and compliance with this Agreement. This accessibility requirement shall include the right to review and copy such records. This requirement includes any auditing, monitoring, and evaluation procedures, including on-site visits performed individually or jointly, by State or Federal Officials or their designees, necessary to verify the accuracy of the Contractor's invoices and compliance with this Agreement. If records are being maintained outside of Rhode Island, such records shall be made accessible by the Contractor at a Rhode Island location. Fiscal records and narrative documents pertaining to activities performed under this Agreement will be retained for audit purposes for a period of at least three (3) years following the submission of the final expenditure report. If audit findings have not been resolved by the end of the three (3) years, the records shall be retained for three (3) additional years after the resolution of the audit findings are made or as otherwise required by law.

If subcontractors are permitted within the scope of this Agreement, the Contractor and its subcontractors will provide and maintain a quality assurance system approved by the State. This system shall cover deliverables and services under this Agreement. It will tender to the State only those deliverables that have been inspected and found to conform to the requirements of this Agreement. The Contractor will keep records evidencing inspections and their results. These records will be made available to the State during the Agreement performance period and for three (3) years after the final payment.

Further, the Contractor agrees to include a similar right of the State to audit records and interview staff, or any subcontractors related to the performance of this Agreement.

PAR. 10. SECURITY AND CONFIDENTIALITY

10.1. Definitions

The following definitions shall apply:

1. The Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") define "**Breach**" as any act of or suspicion of acquisition, access, use, disclosure, of Protected Health Information ("PHI") in violation of HIPAA privacy rules that compromise Personally Identifiable Information ("PII") security or privacy. Additionally, a breach or suspected breach means any actual or suspected possession, access, use, or disclosure of PII or Sensitive Information ("SI")
2. The Office of Management and Budget, Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017), defines "**Incident**" as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system, or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies, without lawful authority.
3. "**Confidential Information**" is defined as any information received or accessed by the Contractor under this Agreement, including PII, SI, PHI, Return Information, or other information, including electronically stored information or records, sufficient to identify an applicant for or recipient of governmental benefits. "Confidential Information" also applies to any preliminary drafts, notes, impressions, memoranda, working papers, and work products of State employees, as well as any other records, reports, opinions, information, and statements required to be kept confidential by the state or federal law or regulation or rule of any court; any statistical, personal technical, and other data and information relating to the State's data, or other such data protected by state and federal laws.
4. "**Personally Identifiable Information**" or "**PII**" (As defined in 45 CFR § 75.2 and OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Technology Investments") is an individual's personal information maintained by an agency, which includes, but is not limited to, education, financial transactions, medical, criminal, or employment history, and information that can be used to distinguish or trace the individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to the specific individual such as their name, social security number, date and place of birth, mother's maiden name, or biometric records. PII shall also include an individual's first name or first initial and last name combined with any one or more type of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date, and place of birth, mother's maiden name, criminal, medical and financial records, or

educational transcripts (as defined in 45 CFR § 75.2 Protected Personally Identifiable Information).

5. **"Protected Health Information" or "PHI"** is defined as identifiable information relating to the past, present, or future health status of an individual, created, collected, transmitted, or maintained by a HIPAA compliant entity as it relates to the provision of healthcare, payment for healthcare services, or use in healthcare operations. Under HIPAA, diagnoses, treatment, medical test results, and prescription information are considered protected health information. Other examples of PHI include National identification numbers, demographic information such as birth dates, gender, ethnicity, contact, and emergency contact information. PHI relates to physical records, whereas ePHI is any PHI created, stored, transmitted, or received electronically. PHI does not include educational or employment records information that involves health information maintained by a HIPAA compliant entity as an employer.
6. **"Return Information"** is defined under 26 USC § 6103(b)(2) and has the same meaning as "Federal Tax Information" or "FTI" as used in IRS Publication 1075.
7. **"Sensitive Information or "SI"** is information that could potentially have a profound, severe, or catastrophic adverse effect on organizational operations, assets, or individuals if the confidentiality, integrity, or availability is lost. Further, the loss of Sensitive Information confidentiality, integrity, or availability might (i) cause significant or severe degradation in mission capability to the extent that the organization is unable to perform its primary functions.
(ii) result in considerable damage to organizational assets; (iii) result in sizable financial loss; or
(iv) result in significant, severe, or catastrophic harm that may involve loss of life or serious life-threatening injuries. (Defined in HHS Memorandum ISP-2007-005, "Departmental Standard for the Definition of Sensitive Information" as amended).

10.2 General

The Contractor shall take security measures to protect against the improper use, loss, access of, and disclosure of any Confidential Information it receives or has access to under this Agreement as required by this Agreement, the RFP and proposal, or which becomes available to The Contractor in carrying out this Agreement. The Contractor agrees to comply with State requirements for safeguarding Confidential Information. All such information shall be held in strict confidence and protected by the Contractor from any unauthorized use and disclosure utilizing the same or more effective procedural requirements as applicable to the State.

10.3 Privacy and Security Safeguards and Obligations

For all Confidential Information under this Agreement, the Contractor must comply with the following privacy and security requirements and obligations:

- a. Ensure that its employees, contractors, and agents implement appropriate administrative, physical, and technological safeguards to protect Confidential Information received by the Contractor under this Agreement from loss, theft, or inadvertent disclosure.
 - i. **Administrative Safeguards:** The Contractor will advise all users with access to the Confidential Information of its confidential nature, the safeguards required to protect such information, and the civil and criminal sanctions for non-compliance with applicable Federal laws.
 - ii. **Physical Security and Storage:** The Contractor will store the Confidential Information in an area that is physically and technologically secure from access by unauthorized persons during duty hours and non-duty hours or when not in use by employing door

locks, keycards, or biometric identifiers. Only authorized personnel will transport the Confidential Information. The Contractor will establish appropriate safeguards for such Confidential Information, as determined by a risk-based assessment of the circumstances involved.

- iii. Technical Safeguards: The Contractor agrees that Confidential Information exchanged under this Agreement will be processed under the immediate supervision and control of authorized personnel. The Contractor will protect the confidentiality of the information so that unauthorized persons cannot retrieve any such Confidential Information utilizing a computer, remote terminal, or any other means. The Contractor personnel must enter personal identification information when accessing Confidential Information on the State's systems. The Contractor will strictly limit authorization to those electronic Confidential Information areas necessary for authorized persons to perform their official duties.
- iv. The Contractor understands that they are responsible for safeguarding this information, regardless of whether or not the Contractor employee, subcontractor, or agent is at their regular duty station.
- v. The Contractor will ensure that laptops and other electronic devices and media containing Confidential Information that constitutes PII are encrypted, and password protected.
- vi. The Contractor will send emails containing Confidential Information that constitutes PII only if encrypted and transmitted to or received by persons authorized to receive such information. In the case of FTI, the Contractor, employees, subcontractors, or agents must comply with the Internal Revenue Service ("IRS") Publication 1075, rules, and restrictions on emailing return information.
- vii. The Contractor will restrict access to the Confidential Information to only authorized employees, subcontractors, and agents that require such Confidential Information to perform their official duties in connection with purposes identified in this Agreement. Minimum restrictions shall include role-based access that limits access to those individuals who need it to perform their official duties in connection with the uses of Confidential Information authorized in this Agreement. ("Authorized Users"). The Contractor shall not use or access Confidential Data for independent projects unrelated to the purposes identified in this Agreement. The Contractor shall advise all users with access to the Confidential Information of the confidential nature of the information and the safeguards required to protect it. Further, the Contractor shall inform authorized users of the civil and criminal sanctions for non-compliance with applicable Federal Laws. The Contractor shall require all its employees, subcontractors, and agents with authorized access to the Confidential Information disclosed to comply with the terms and conditions outlined in this Agreement and not duplicate, disseminate, or disclose such Confidential Information unless authorized under this Agreement.
- viii. For receipt of FTI, the Contractor agrees to maintain all Return Information sourced from the IRS in accordance with IRS section 6103(p)(3) and comply with the safeguards and requirements set forth in Publication 1075, "Tax Information Security Guidelines for Federal, State, and Local Agencies." According to the IRS published guidance for security guidelines and other safeguards for protecting Return Information per 26 CFR § 301.6103(p)(4)-1, the Contractor shall:
 - (1) Establish a central point of control for all requests for and receipt of Return Information and maintain a record to account for all subsequent dissemination and products utilizing that information and movement of the data until

destroyed, per Publication 1075.

- (2) Establish procedures for secure storage of Return Information that consistently maintain two layers of protection to prevent unauthorized access to the information, including when in transit, per Publication 1075.
- (3) Accurately label Return Information obtained under this Agreement to be identifiable and restrict unauthorized individuals' access. Any Duplication or transcription of Return Information used to create new records must also be appropriately accounted for and safeguarded. Return Information should not be merged with other documents unless the entire file is protected in the same manner as is required for Return Information, and the FTI within it is clearly identified in accordance with Publication 1075.
- (4) Restrict access to Return Information exclusively to officers, employees, agents, and subcontractors, which require access to carry out this Agreement. Before permitting access to Return Information, the Contractor must evaluate which personnel requires such access on a need-to-know basis. Authorized individuals may only access Return Information to the extent necessary to perform services related to this Agreement, per Publication 1075.
- (5) Prior to initial access to FTU and annually after that, the Contractor will ensure that employees, officers, agents, and subcontractors that will have access to Return Information receive awareness training regarding the confidentiality restrictions applicable to the Return Information and certify acknowledgment in writing that they are aware of the criminal penalties and civil liabilities provided by sections 7213, 7213A, and 7431 of the Internal Revenue Code for any willful disclosure or inspection of Return Information that is not authorized by the Internal Revenue Code, per Publication 1075.
- (6) Ensure that systems processing Return Information are compliant with Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act of 2002 (FISMA).

10.4 Ownership of Confidential Information

Confidential Information provided to or transferred by the State to which the Contractor has access for the performance of this Agreement, is the sole property of the State. The Contractor agrees and acknowledges that the Confidential Information shall not be disclosed, used, misused, provided to, or accessed by any other individual, entity, or party without the express written consent of the State. Further, the Contractor expressly agrees to immediately return any Confidential Information or Confidential Information Database upon the State's written request or cancellation or termination of this Agreement.

10.5 Compliance with Applicable Laws, Regulations, Policies, and Standards

The Contractor agrees to abide by all applicable, current, or as amended Federal and State laws, regulations, policies, guidance, and standards governing the confidentiality of information it may have access to under this Agreement, including, but not limited to, the Business Associate requirements of HIPAA (www.hhs.gov/ocr/hipaa) and 45 CFR § 155.260. Additionally, the Contractor agrees to comply with the State confidentiality policy recognizing a person's fundamental right to privacy and confidentiality of personal information.

The Contractor agrees to adhere to all applicable State and Federal statutes and regulations relating to personal health care and substance use treatment, including but not limited to the

Federal Regulation 42 CFR, Part 2; Rhode Island Mental Health Law, RI General Laws Chapter 5-37.3-1 et seq; Identity Theft Protection Act of 2015, Rhode Island General Laws Chapter 11-49.3 and HIPAA and its implementing regulations. The Contractor acknowledges that failure to comply with the provisions of this Paragraph (10.5) will result in the termination of this Agreement.

In connection with all PII that the Contractor receives or has access to under this Agreement, the Contractor must comply with Minimum Acceptable Risk Standards for Exchanges ("MARS-E"), version 2.0, dated November 15, 2015, which includes the following suite of documents: Volume I: Harmonized Security and Privacy Framework; Volume II: Minimum Acceptable Risk Standards for Exchanges; Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges; and Volume IV: ACA Administering Entity System Security Plan.

Notwithstanding any other requirements outlined in this Agreement, the Contractor acknowledges and agrees to the regulations imposed and requirements concerning privacy, security, and breach notification per the HITECH Act and its implementation. The Contractor shall implement such conditions by rules adopted by the United States Department of Health and Human Services (DHS). The HITECH requirements, regulations, and provisions referenced and outlined herein are hereby incorporated into this Agreement in their entirety. Notwithstanding anything contrary or any condition that may be more restrictive within this Agreement, all requirements and provisions of HITECH and its implementing regulations currently in effect and promulgated and implemented after this Agreement are automatically executed effective and incorporated herein. If this Agreement requires stricter guidelines than those outlined in HITECH, the more stringent guidelines will take precedence.

10.6 Breach/Incident Reporting

Upon notice of a suspected or confirmed Incident or Breach, the State and the Contractor will jointly develop an Incident investigation and remediation plan. Depending on the nature and severity of the confirmed breach, the procedure may include using an independent third-party security firm to perform an objective security audit per cyber security industry commercially reasonable practices. The Parties will consider the scope, severity, and impact of the Incident to determine the extent and duration of the third-party audit. If the Parties cannot agree on the need or scope of such an audit, the matter will be escalated to senior officials of each organization for resolution. The Contractor will incur the costs of all such audits. Depending on the nature and scope of the Incident, remedies may include information to individuals on obtaining credit reports and notification to applicable credit card companies, notice to the local office of the Secret Service, affected users, and other relevant Parties. On a selected basis, the utilization of a call center and the offer of credit monitoring services may be included.

10.7 Other

Failure to abide by the State's confidentiality policy or a required signed Business Associate Agreement ("BAA") will result in termination remedies, including but not limited to termination of this Agreement. A BAA shall be signed by the Contractor, simultaneously or as soon as possible, from the signing of this Agreement, as required by the State. The Contractor agrees that no findings, listings, or information derived from the performance of this Agreement may be released or publicly disclosed in any form or for any purpose if such information contains any combination of data elements that might allow an individual to determine a beneficiary's

identification without first obtaining written authorization from the State's Contract Manager. Examples of such data elements include, but are not limited to geographic indicators, age, sex, diagnoses, procedures, date of birth, or admission or discharge date. The Contractor further agrees that the State shall be the sole judge as to whether any finding, listing, or information extracted or derived from the State's files would identify or, with reasonable effort, permit one to identify or to deduce the identity of an individual with a fair degree of certainty. The Contractor agrees that the conditions set forth herein apply to any materials presented, reviews submitted, or publications that contain individual identifying information unless such information is shown in the aggregate. The Contractor shall not publicly disclose, present, or submit any materials for review or publication that contains an individual's social security number, in part or whole, under any circumstances. The Contractor is hereby notified that all initial data received from the United States Department of Health and Human Services (DHS) is considered confidential by the State.

The Contractor will inform the State of any change in its administrative, technical, or operational environment that would impact compliance with the terms of this Agreement, including but not limited to compliance with 45 CFR§ 155.260.

The Contractor shall monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls following 45CFR § 155.260(a)(5). Under the provisions of this Paragraph (10), the Contractor shall not be required to maintain the confidentiality of Confidential Information that becomes legitimately publicly available or is rightfully obtained from third parties under no obligation of confidentiality.

The Contractor shall establish and maintain policies and procedures to ensure the safekeeping of Confidential Information and prevent unauthorized access to use of such Confidential Information under this Agreement. The Contractor shall comply with ISO 27001 and ISO 27002 (or any replacement standard relating to information security) and applicable regulatory requirements and remain consistent with industry standards. In addition to its other obligations outlined in this Agreement, whenever the Contractor possesses, stores, processes, or has access to the State's Confidential Information, the Contractor shall comply with those information security policies and procedures reasonably required by the State from time to time.

Nothing herein shall limit the State's ability to seek injunctive relief or any damages resulting from the Contractor's negligent or intentional disclosure of Confidential Information.

PAR. 11. NONDISCRIMINATION IN EMPLOYMENT AND SERVICES

By signing this Agreement, the Contractor agrees to comply with the requirements of Title VI of the Civil Rights Act of 1964 (42 USC 2000d et seq.); Section 504 of the Rehabilitation Act of 1973, as amended (29 USC 794); the Americans with Disabilities Act of 1990 (42 USC 1201 et seq.); Title IX of the Education Amendments of 1972 (20 USC 1681 et. Seq.); The Age Discrimination Act of 1975, The United States Department of Health and Human Services (DHHS) Regulations found in 45 CFR, Parts 80 and 84; the United States Department of Education Implementing Regulations (34 CFR, Parts 104 and 106; and BHDDH Directive 1124, which prohibits discrimination based on race, national origin (limited English proficiency persons), age sex (including gender identity, transgender status, sexual orientation, and pregnancy), disabilities, genetic information, marital status, parental status, religion, political beliefs, or retaliation for opposing discriminatory practices for participating in the discrimination-complaint process, in

acceptance of or provision of services, employment, or treatment in educational or other programs or activities, or as any of the Acts are amended from time to time.

Within thirty-five (35) days of the date of a request by DHHS or BHDDH, the Contractor must submit complete information on Title VI and Section 504 compliance or self-assessments, as referenced above, by a subcontractor or vendor of the Contractor.

The Contractor further agrees to comply with all other provisions applicable to law, including the Americans with Disabilities Act of 1990, the Governor's Executive Order No. 05-01, Promotion of Equal Opportunity, and the Prevention of Sexual Harassment in State Government.

The Contractor also agrees to comply with the State's requirements for safeguarding client information as such requirements are made known to the Contractor at the time of this Agreement. Changes to any of the provisions contained herein shall constitute a change and be handled in accordance with 220-RICR-30-00- 13.4(C)(1)(c).

Failure to comply with this Paragraph may be the basis for cancellation or termination of this Agreement.

PAR. 12. MODIFICATION OF AGREEMENT

All modifications to the Agreement are subject to 220-RICR-30-00-13.4(C)(1)(c).

PAR. 13. INTEREST OF CONTRACTOR

The Contractor agrees that it presently has no pecuniary interest and shall not acquire any such claim, direct or indirect, without first disclosing it to the State in writing and then subsequently obtaining approval, in writing, from the State that would conflict in any manner with the performance of services required under this Agreement. The Contractor further agrees that no person having any such interest shall be employed by the Contractor to perform any work associated with this Agreement.

PAR. 14. OWNERSHIP

All data, technical information, information systems, materials gathered, originated, developed, prepared, modified, used, or obtained by the Contractor in the performance of the Agreement, including, but not limited to, all hardware, software, computer programs, data files, application programs, intellectual property, source code, documentation, and manuals, regardless of the state of completion, shall be deemed to be owned and remain owned by the State ("State Property"). Each party will retain all rights to any software, ideas, concepts, expertise, development tools, techniques, or any other proprietary material or information owned or developed before this Agreement or acquired or developed after the date of this Agreement without reference to or use of the intellectual property of the other party. All software licensed by a third-party vendor will be and remain the property of such vendor.

PAR. 15. NOTICES

No notice, approval, or consent permitted or required to be given by this Agreement will be adequate unless the same is in writing and sent postage prepaid, certified mail or registered mail, return receipt requested, or by reputable overnight delivery service to the other party at the address set forth below, or such other address as either party may direct by notice given to the other as

provided, and shall be deemed to be given when received by the addressee.

Contractor:

State of Rhode Island, Department of Behavioral Healthcare, Developmental Disabilities, & Hospitals

PAR. 16. GOVERNING LAW

This Agreement is deemed executed and delivered in the City of Cranston, State of Rhode Island. The State of Rhode Island laws shall govern all questions arising from or under this Agreement.

PAR. 17. INSURANCE

Throughout the term of this Agreement and any extended periods, Insurance Requirements for Professional Services, the Contractor, and any subcontractor shall procure and maintain, at its own cost and expense, insurances as required by Addendum A, General Conditions of Insurance, per the State of Rhode Island, Division of Purchases ([Procurement Statutes and Regulations | Rhode Island Division of Purchases \(ri.gov\)](http://Procurement Statutes and Regulations | Rhode Island Division of Purchases (ri.gov)))

IN WITNESS WHEREOF, the Parties hereto and hereunder set their hands as of the date of this Agreement made legally binding upon the issuance of a valid Purchase Order by the State of Rhode Island as follows:

Vendor Name	State of Rhode Island, Department of Behavioral Healthcare, Developmental Disabilities, & Hospitals
--------------------	--

Director

Title of Authorized Agent

Title of Authorized Agent

Printed Name of Authorized Agent

Richard Leclerc

Printed Name of Authorized Agent

Signature of Authorized Agent

Signature of Authorized Agent

Date

Date

EXHIBIT A
SCOPE OF WORK

EXHIBIT B
BUDGET

EXHIBIT C
PAYMENTS AND REPORTS SCHEDULE

- **Payments**

- Payments are made upon receipt of invoice. Invoices will be reviewed and approved by BHDDH Finance. Vendors shall submit invoices by the 15th day of the following month.
- Invoices must be based upon the approved Budget in Exhibit B.
 - Any budget changes must be made and approved in writing or via the program manager before any spending. The Contractor agrees not to submit invoices based on proposed budget changes before written approval.
 - Invoices will be paid for services rendered *or* on a reimbursement basis. The Contractor will only submit invoices for work performed or for expenses already paid and seek reimbursement from The Department.
 - All monthly payment requests must include detailed supporting documentation for employee's wages and fringe benefits.
- The Department currently operates on a "NET 30" basis for payments, meaning payment cannot be made until 30 days after the billing period or 30 days from the date the Department receives the invoice. (Example, if an invoice is submitted on March 15th for February services, it cannot be paid until April 15th.)
- The Department reserves the right to request backup to any submitted invoice before payment at any time. Failure to provide this invoice promptly may result in non-payment.

EXHIBIT D OIG-HHS EXCLUSION LIST

According to the Social Security Act 1128, 1128B (f) (1), 42 CFR- Public Health, Chapter V, OIG, HHS, Part 1000, The State of Rhode Island is obligated to direct Medicaid providers to screen their employees and contractors for excluded persons based on the authority contained in various sections of the Social Security Act. When HHS-OIG has excluded a provider, Federal health care programs (Medicaid and SCHIP) are prohibited from paying for any items or services furnished, ordered, or prescribed by excluded individuals or entities. This payment ban applies to any items or services reimbursable under a Medicaid program delivered by an excluded individual or entity.

All providers in the Medicaid program must take the following steps to determine whether their employees and contractors are excluded individuals or entities:

1. Prior to employment, screen all employees and noncontractors to determine whether any of them have been excluded.
2. Search the HHS-OIG website by the names of any individuals or entity (HHS-OIG maintains the LEIE, a database accessible to the general public that provides information about parties excluded from participation in Medicare, Medicaid, and other Federal health care programs.
The LEIE website is located at <http://www.oig.hhs.gov/fraud/exclusions.asp>.
3. Search the HHS-OIG website quarterly to capture exclusions and reinstatements that could have occurred since the last search.
4. Search the Excluded Parties List System (EPLS) website by the names of an individual or entity. The EPLS website includes information regarding entities debarred, suspended, proposed for debarment, excluded or disqualified under the non-procurement common rule, or otherwise declared ineligible from receiving Federal contracts, certain subcontracts, and certain Federal assistance and benefits.
The EPLS website is located at <https://www.epls.gov/>.
5. Immediately report any exclusion information discovered to the Rhode Island Executive Office of Health and Human Services.

Civil monetary penalties may be imposed against Medicaid providers who employ or enter into contracts with excluded individuals or entities to provide items or services to Medicaid recipients.

EXHIBIT E FALSE CLAIMS ACT

(A) **Definitions**

Abuse - Practices that are inconsistent with accepted sound fiscal, business, or medical practices, and result in an unnecessary cost or reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care, such as, but not limited to:

- Misusing codes on a claim,
- Billing for services that were not medically necessary.

Federal False Claims Act (FCA) - A federal law that prohibits the submission of false information, records or claims for payment to the federal government. The FCA is a federal law that imposes liability on persons or entities that defraud the government. The FCA prohibits anyone from knowingly presenting, or causing to be presented, a false or fraudulent claim for payment or approval or knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent claim.

A violation of the False Claims Act can result in severe financial penalties. Examples of false claims include (but is not limited to) billing for services not provided or not medically necessary, billing for the same services more than once, charging excessively for services or supplies or making false statements to receive payment for services.

Fraud - Generally defined as knowingly and willfully executing or attempting to execute or artifice to defraud any healthcare benefit program or to obtain (by means of false or fraudulent pretenses, representation or promises) any of the money or property owned by, or under the custody or control of, any healthcare benefit program. (18 U.S.C. §1347)

Knowing / Knowingly - A person has (i) actual knowledge that the information is false, (ii) acts with deliberate indifference to whether the information is true or false, or (iii) acts in “reckless disregard” of whether the information is true or false. The False Claims Act does not require proof of actual intent to defraud.

State of R.I. False Claims Act - § 9-1.1-3. - A state law modeled after the federal False Claims Act that prohibits the submission of false information, records or claims for payment. It is a state law that imposes liability on persons or entities that defraud the government. It is the prohibition of knowingly presenting, or causing to be presented, a false or fraudulent claim for payment or approval or knowingly making, using, or causing to be made or used, a false record or statement material to a false or fraudulent claim, the misappropriation of state property, or deceptively avoiding binding obligations to pay the state, among other violations.

A violation of the state False Claims Act can result in severe financial penalties. Examples of false claims include billing for services not provided or not medically necessary, billing for the same services more than once or making false statements to receive payment for services.

Waste - Overutilization of services or other practices that, directly or indirectly, result in unnecessary costs to the healthcare system, including the Medicare and Medicaid programs. It is not generally considered to be caused by criminally negligent actions but by misuse of resources.

Examples of waste include, but is not limited to:

- (i) spending on services that lack evidence of producing better health outcomes compared to less expensive alternatives
- (ii) inefficiencies in the provision of healthcare goods and services or
- (iii) Costs incurred while treating avoidable medical injuries, such as preventable infections in hospitals

The Contractor hereby certifies that they have read and agree to the policy set forth in the Federal False Claims Act.

Contractor Signature: _____

Contractor Title: _____

Date: _____

E. Related Policies HR-FRAUD-2010
F. Reference(s) RIGL § 36.14.1
Personnel Rule 6.02 RIGL § 9-1.1-3.

EXHIBIT F
RHODE ISLAND WHISTLEBLOWER PROTECTION ACT

Whistleblower - People who report or disclose information about actual or suspected illegal, unethical, or improper conduct in their workplace or organization. Whistleblowers have certain rights and protections under the law, depending on the nature and scope of their disclosure.

In Rhode Island, whistleblowers have rights under the Rhode Island Whistleblowers' Protection Act, which applies to both public and private employees. This law prohibits employers from firing, threatening, or discriminating against an employee who reports, or refuses to participate in, any activity that violates the law, regulations, or public policy. The law also protects employees who testify or assist in any investigation or proceeding related to such activity.

(B) Policy

The Department of Behavioral Healthcare, Developmental Disabilities and Hospitals (BHDDH) and Eleanor Slater Hospital (ESH or hospital) are committed to ensuring compliance with Federal and State laws and regulations that prohibit fraud, waste, and abuse. ESH is committed to enforcing procedures to detect and prevent fraud, waste, and abuse in receiving payments from federal health care programs. The hospital is equally committed to educating and training staff about fraud and abuse, the provisions of the federal and state False Claims Acts and their civil penalties, as well as protecting the rights of those who report or disclose information about actual or suspected illegal, unethical, or improper conduct in the workplace or organization.

(C) Procedures

1. All workforce members, management and contractors or agents will be educated on the laws regarding false or fraudulent claims, either through education or training or through provisions contained in contracts and agreements.

2. Compliance Officer

There shall be a Compliance Officer who is responsible for ensuring that the compliance program is effective in detecting and preventing potential incidents of fraud, waste, and abuse.

The Compliance Officer will oversee managers who will establish and maintain methods for detecting and preventing incidents of fraud, waste, and abuse, including but not limited to:

- (i) A claims quality assurance program that monitors the accuracy of adjudicated claims,
- (ii) A compliance hotline to report suspected fraud, waste, and abuse,
- (iii) A process that identifies employees, contractors, vendors, and providers that are debarred or excluded from participating in federal programs.

The Compliance Officer shall ensure that any incidents are appropriately handled by qualified personnel, discussed, and reported to appropriate law enforcement agencies.

If there is a determination that there has been an incident of fraud, waste and/or abuse, the Compliance Officer shall ensure that the hospital implements systematic changes and corrective action initiatives to prevent further offenses.

The Compliance Officer shall ensure that the hospital cooperates with all federal and state agencies that conduct health care fraud and abuse investigations.

The Compliance Officer shall, in consultation with legal counsel, be responsible for receiving and acting upon all information suggesting possible fraud, abuse or wrongdoing, and for directing all investigations.

The Compliance Officer shall, in consultation with legal counsel, be responsible for conducting investigations into any allegations of suspected violations of any criminal, civil or administrative law. In doing the investigation, the Compliance Officer, or their designee, will gather the facts of the alleged incident as promptly as possible.

If the Compliance Officer determines that there is sufficient evidence to support an allegation of violation of law or regulation, he/she will consult with legal counsel on further investigation, and whether legal counsel should conduct or direct additional investigations. If an allegation is a criminal violation of law, the Compliance Officer will immediately refer the case to legal counsel. Legal counsel will evaluate the facts and determine if credible evidence of a violation of civil, criminal or administrative law exists. Legal counsel will notify the Compliance Officer and senior management of its determination, and the Compliance Officer shall act accordingly with referrals to outside investigative agencies, Human Resources, and any other reporting entity.

The Compliance Officer and the legal department will determine the extent of the potential liability resulting from the false claims submission, and both will assist in the planning and appropriate actions to correct the deficiencies and resolve any liability issues. These tasks shall be the responsibility of the Compliance Officer, with input from the legal department.

The Compliance Officer shall, to the extent possible, maintain the confidentiality or anonymity of any staff person who makes a report of suspected fraud, waste and/or abuse if the staff person so requests.

The Compliance Officer shall be responsible for ensuring that all workforce members are trained on the False Claims Act and Whistleblower protections afforded to staff who report suspected or potential incidents of fraud, abuse and/or other wrongdoing. The training shall include:

- (i) Detailed information on the federal and state False Claims Acts and the administrative solutions for false claims and statements,
- (ii) Federal and state laws pertaining to civil or criminal False Claims Act penalties,
- (iii) Whistleblower rights and protections
- (iv) The Departments requirements for preventing, detecting, and reporting fraud, waste, and abuse.

3. Staff, workforce members, management, contractors, and agents

Staff, workforce members, management, contractors, and agents shall:

- (i) Conduct themselves in an ethical and legal manner, including maintaining accurate records related to the rendering of items or services payable by federal health care programs.
- (ii) Be responsible for reporting potential or suspected incidents of fraud and abuse and/or other wrongdoing directly to their supervisor and/or executive management through any of the following means:

- i. To their direct supervisor
 - ii. To any supervisor or member of management
 - iii. To Human Resources
 - iv. To the Compliance Officer or Compliance Department
 - v. To the confidential hotline (Lighthouse)
- (iii) Employees that report suspected violations of the False Claims Act for which the hospital or Department does not investigate or does not remediate, may make a report to the federal government as a Whistleblower.

Any party who receives a report of fraud who is not the Compliance Officer shall immediately inform the Compliance Officer who will be responsible for the initial investigation. No supervisor or member of management should directly confront the person alleged to have committed the fraud, waste, or abuse, or otherwise discuss the issue with anyone suspected of engaging in fraudulent or abusive practices without prior approval from the Compliance Officer.

4. Department/Hospital

The Department/hospital will take appropriate disciplinary and enforcement action (i.e., plans of correction, employee discipline or termination, termination of a contract or agreement) against any workforce members, providers, contractors, consultants, agents, etc. found to have committed fraud, abuse, waste and/or wrongdoing.

5. Whistleblower Protection

Retaliation and/or retribution for reporting issues in good faith is prohibited. The Department and hospital will protect all workforce members from retaliation and retribution when they make a good faith report of suspected wrongdoing through any reporting method.

Whistleblowers who report fraud or false claims against the state government have rights under the Rhode Island False Claims Act, which allows them to file a lawsuit on behalf of the state and receive a share of the recovery if the case is successful. The law also protects whistleblowers from retaliation by their employers or contractors for bringing or assisting in such a lawsuit.

Whistleblowers who file a complaint or testify before the Rhode Island Ethics Commission have rights under the Rhode Island Whistleblower Act, which protects them from being threatened or intimidated by anyone involved in the proceeding. The law also allows them to bring a civil action in Superior Court within three years if they suffer any retaliation.

Whistleblowers who report wrongdoing in the workplace have rights under the common law of Rhode Island, which recognizes a public policy exception to the at-will employment doctrine. This means that an employer cannot fire an employee for a reason that violates a clear and substantial public interest, such as reporting illegal or unsafe conduct, or exercising a legal right or duty.

Whistleblowers have the right to seek legal advice and representation from an attorney who specializes in whistleblower law. An attorney can help whistleblowers understand their rights and options and assist them in pursuing their claims and remedies.

B. Penalties and fines

Violations of the False Claims Act that include fraud, waste and abuse may result in any or all of the following:

- a. Civil monetary penalties: Payment of interest at the maximum rate on the amount of the payments, a fine between five thousand five hundred dollars (\$5,500) and eleven thousand dollars (\$11,000) for each false filing, and any other reasonable expenses determined by the court.
- b. Fines: In addition to five thousand five hundred dollars (\$5,500) to eleven thousand dollars (\$11,000) for each act, an assessment of damages three times the amount of the overpayment may be prescribed.
- c. Criminal penalties: If convicted, the individual could face jail time and be ordered to pay fines and restitution. Additionally, a licensure could come under review and be suspended or permanently revoked.
- d. Medicare/Medicaid Exclusion: A conviction under the False Claims Act could lead to exclusion from Medicare, Medicaid, and all other Federal health care programs. If excluded, then no payment will be made by any Federal health care program for any items or services furnished, ordered, or prescribed by an excluded individual or entity.
- e. Health care providers and suppliers (person and organizations) who violate the False Claims Act are subject to an investigation by the Office of Inspector General (OIG), who may seek to exclude the provider or supplier from participation in federal health care programs.

The Contractor hereby certifies that they have read and agree to the policy set forth in The Rhode Island Whistleblowers' Protection Act.

Contractor Signature: _____

Contractor Title: _____

Date: _____

C. Related Policies HR-FRAUD-2010
D. Reference(s) RIGL § 36.14.1
Personnel Rule 6.02 RIGL § 9-1.1-3.