



**State of Rhode Island  
Department of Administration / Division of Purchases  
One Capitol Hill, Providence, Rhode Island 02908-5855  
Tel: (401) 574-8100 Fax: (401) 574-8387**

**Solicitation Information  
April 16, 2013**

**ADDENDUM # 4**

**RFP #7461348**

**RFP Title: Rhode Island Health Insurance Contact Center**

**Bid Opening Date & Time: Monday, April 22, 2013 @ 11:00 AM (EST)**

---

**Notice to Vendors:**

ATTACHED ARE APPENDICES E AND F

**David J. Francis  
Interdepartmental Project Manager**

*Interested parties should monitor this website, on a regular basis, for any additional information that may be posted.*

## APPENDIX E

### **Instructions for Certification Regarding Debarment, Suspension, and Other Responsibility Matters — Primary Covered Transactions and Certification**

1. By signing and submitting the proposal, the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. If necessary, the prospective participant shall submit an explanation of why it cannot provide the certification. The certification or explanation will be considered in connection with the determination by the Office of the Governor, Division of the Rhode Island Health Benefits Exchange (the "Exchange") whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. This certification is a material representation of fact upon which reliance will be placed when the Exchange determines whether to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Exchange, the Exchange may terminate this transaction for cause or default.
4. The prospective primary participant shall provide immediate written notice to the Exchange if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the definitions and coverage sections of the rules implementing executive order: 12549: 45 CFR Part 76.
6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the Exchange.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause title "Certification regarding debarment, suspension, ineligibility and voluntary exclusion - lower tier covered transactions, provided by the Exchange, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of prospective participant in a lower tier covered transaction that is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List.
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by

this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under Paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the federal government, the department may terminate this transaction for cause of default.

**Certification Regarding Debarment, Suspension, and Other Responsibility Matters  
Primary Covered Transaction**

(1) The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;

(b) Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(c) Are not presently indicted for otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraph (1) (b) of this certification; and

(d) Have not within a three-year period preceding this application/proposal had one or more public transactions (federal, state, or local) terminated for cause or default.

(2) Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

---

Authorized Agent/Signature

Date

## APPENDIX F

### BUSINESS ASSOCIATE AGREEMENT ADDENDUM

Except as otherwise provided in this Business Associate Agreement Addendum, \_\_\_\_\_ (insert name of Business Associate), (hereinafter referred to as "Business Associate"), may use, access or disclose Protected Health Information (as defined below) to perform functions, activities or services for or on behalf of the Division of the Rhode Island Health Benefits Exchange in the Office of the Governor (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", as further defined below), 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, parts 160, 162 and 164, hereinafter referred to as the Privacy and Security Rules and patient confidentiality regulations contained therein, and the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009, 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, R.I. General Laws Chapter 40.1-5-26, and Confidentiality of Health Care Communications and Information Act, R.I. General Laws Chapter 5-37.3-1 *et seq.* Business Associate recognizes and agrees it is obligated by law to meet the provisions of the HITECH Act applicable to Business Associate in its performance of services under the Agreement.

#### 1. Definitions

- A. "Addendum" means this Business Associate Agreement Addendum.
- B. "Agreement" means the contractual Agreement by and between the State of Rhode Island, **Executive Office of Health and Human Services** and Business Associate, awarded pursuant to 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. "Breach" means the acquisition, access, use or disclosure of Protected Health Information (PHI) in a manner not permitted under HIPAA (45 CFR Part 164, Subpart E) which compromises the security or privacy of the Protected Health Information. For the purposes of the HITECH Act, a Breach shall not include:
  - i. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the Covered Entity or the Business Associate, if such acquisition, access or use was made in good faith and within the course and scope of authority and employment, and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or,

ii. Any inadvertent disclosure by a person who is authorized to access PHI at Covered Entity or Business Associate to another person authorized to access PHI at Covered Entity or Business Associate, respectively, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or,

iii. A disclosure of PHI where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

D. The lower case term "business associate" means with respect to a covered entity, a person who:

i. On behalf of such Covered Entity, but other than in the capacity of a member of the workforce of such Covered Entity performs or assists in the performance of:

a. a function or activity involving the use or disclosure of Personally Identifiable Health Information, including claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or,

b. any other function or activity regulated by the HIPAA Privacy Rule or HIPAA Security Rule;

ii. Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for such Covered Entity where the provision of the service involves the disclosure of Personally Identifiable Health Information from such Covered Entity to the person.

E. "Client/Patient" means a Covered Entity funded person who is the subject of the Protected Health Information.

F. The lower case term "covered entity" means a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy Rule and the Security Rule.

G. "Data Aggregation" means, with respect to PHI created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such PHI by the business associate with the PHI received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

H. "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed or consulted by authorized health care clinicians and staff.

I. "Electronic Protected Health Information" or "Electronic PHI" means PHI that is transmitted by or maintained in electronic media as defined in the HIPAA Security Rule.

J. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

K. "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 at 45 CFR Part 160 and 45 CFR Part 164, Subpart A and Subpart E.

L. "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 XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 ("ARRA"), and any regulations promulgated thereunder and as amended from time to time.

M. "Personally Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and:

i. is created or receive by a health care provider, health plan, employer or health care clearinghouse; and,

ii. relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and,

a. that identifies the individual; or

b. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

N. "Protected Health Information" or "PHI" means Personally Identifiable Health Information transmitted or maintained in any form or medium in connection with the Agreement that:

i. is received by Business Associate from Covered Entity;

ii. Business Associate creates for its own purposes from Personally Identifiable Health Information that Business Associate received from Covered Entity; or,

iii. is created, received, transmitted or maintained by Business Associate on behalf of Covered Entity.

Protected Health Information excludes Personally Identifiable Health Information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. Section 1232(g), records described at 20 U.S.C. Section 1232g(a)(4)(B)(iv), and employment records held by the Covered Entity in its role as employer.

O. "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.

P. "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 in an information system.

Q. "Security Rule" means the Standards for the security of Electronic Protected Health Information found at 45 CFR 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 Business Associate of Covered Entity in the same manner that such sections apply to the Covered Entity.

R. "Suspected breach" is a suspected acquisition, access, use or disclosure of Protected Health Information in violation of the HIPAA Privacy Rule, as referenced above, that compromises the security or privacy of such PHI.

S. "Unsecured PHI" means PHI that is not secured, as specified in 45 CFR 164.402, through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services.

T. "Vendor of Personal Health Records" shall mean an entity, other than a covered entity, that offers or maintains a personal health record.

U. Any terms capitalized, but not otherwise defined, in the Addendum shall have the same meaning as those terms have under HIPAA, the HIPAA Privacy Rule, the HIPAA Security Rule and the HITECH Act.

## **2. Obligations and Activities of Business Associate**

### **A. Permitted Uses.**

i. PHI Described. PHI disclosed by the Covered Entity to the Business Associate, PHI created by the Business Associate on behalf of the Covered Entity, and PHI received by the Business Associate from a third party on behalf of the Covered Entity are disclosable under this Addendum. The disclosable PHI is limited to the extent practicable, to the Limited Data Set of such PHI (as defined in 45 C.F.R. § 164.514(e)(2)), or, if the disclosure of PHI, not in a Limited Data Set, is necessary for Business Associate's performance under the Agreement, limited to the minimum necessary to complete the tasks, or to provide the services, associated with the terms of the original Agreement; provided, however, that the requirements set forth above in this subsection (i) shall be superseded and replaced by the requirements of the "minimum necessary" regulations or guidance to be issued by the Secretary (pursuant to 42 U.S.C. § 17935(b)(1)(B)).

ii. Purposes. Except as otherwise limited in this Addendum, Business Associate may use or disclose the PHI on behalf of, or to provide services to, Covered Entity for the purposes necessary to complete the tasks, or provide the services,

associated with, and required by the terms of the Agreement, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Covered Entity or violate the HIPAA Privacy Rule if done by the Covered Entity. Business Associate shall limit any disclosure or use of PHI to its employees, subcontractors, agents, or other third parties, and request from Covered Entity, to the extent practicable, to the Limited Data Set of such Protected Health Information (as defined in 45 C.F.R. § 164.514(e)(2)), or, if the disclosure, request, or use by Business Associate PHI, not in a Limited Data Set, is necessary for Business Associate's performance of services under the Agreement, Business Associate will limit the amount of such PHI disclosed, requested or used to only the minimum PHI necessary to perform or fulfill a specific function required or permitted under the Agreement; provided, however, that the requirements set forth above in this subsection (ii) shall be superseded and replaced by the requirements of the "minimum necessary" regulations or guidance to be issued by the Secretary (pursuant to 42 U.S.C. § 17935(b)(1)(B)).

B. Prohibited Uses and Disclosures. Business Associate shall not use PHI in any manner that would constitute a violation of the HIPAA Privacy Rule or the HITECH Act.

i. Stated Purposes Only. The Business Associate shall not use the PHI for any purpose other than stated or permitted in the Agreement, this Addendum or as Required or permitted by Law.

ii. Limited Disclosure. The PHI is confidential and will not be disclosed by the Business Associate other than as stated or permitted in this Addendum or as Required or permitted by Law. Business Associate will refrain from receiving any remuneration in exchange for any individual's PHI, unless Covered Entity gives written approval, and the exchange is pursuant to a valid authorization (that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual), or satisfies one of the exceptions enumerated in Section 13405(e)(2) of the HITECH Act. Business Associate will refrain from marketing activities that would violate HIPAA, specifically Section 13406 of the HITECH Act. Business Associate will report to Covered Entity any use or disclosure of the PHI, including any Security Incident affecting PHI not provided for by this Addendum of which it becomes aware.

C. Appropriate Safeguards. Business Associate shall implement the following administrative, physical, and technical safeguards in accordance with the Security Rule under 45 C.F.R., Sections 164.308, 164.310, 164.312 and 164.316:

i. Implement policies and procedures designed to prevent, detect, contain and help correct information security violations; identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the Business Associate; implement an appropriate security awareness and training program for all members of its workforce; implement policies and procedures designed to prevent those workforce members who are not authorized to have access from obtaining access to electronic PHI; implement policy and procedures to address Security Incidents; establish policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic PHI; and perform a

periodic technical and non-technical evaluation in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which the security policies and procedures of Business Associate (and any agent of Business Associate) meet its requirements.

ii. Implement policies and procedures designed to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed; implement policies and procedures that specify the proper functions to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic PHI; implement appropriate physical safeguards for all workstations that access electronic PHI; restrict access to authorized users; implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility and the movement of these items within the facility.

iii. Implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights as specified in 45 C.F.R., Section 164.308; implement appropriate hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI; implement policies and procedures designed to protect electronic PHI from improper alteration, destruction, unauthorized access or loss of integrity or availability.

iv. The Business Associate will use appropriate safeguards to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to the limitation of the groups of its employees or agents, otherwise known as workforce members, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum.

v. Business Associate shall ensure that any agent, contractor, subcontractor, etc., to whom Business Associate provides such PHI, agrees to implement reasonable and appropriate safeguards to protect such PHI.

vi. Appropriate notification and training of its employees or agents to whom the PHI will be disclosed designed to protect the PHI from unauthorized disclosure. At the sole discretion of the Business Associate: provide a written statement to each employee or agent as to the necessity of maintaining the security and confidentiality of Protected Health Information, and of the penalties provided for the unauthorized release, use, or disclosure of this information; Receipt of the statement is to be acknowledged by the employee or agent, who is to sign and return the statement to his or her employer or principal, who then is to retain the signed original; The employee or agent is also to be furnished with a copy of the signed statement; The Business Associate shall take no disciplinary or punitive action against any employee or agent solely for bringing evidence of violation of the referenced security requirements to the attention of the Covered Entity.

vii. A copy of the above-described policies, procedures and documentation shall be provided to the Covered Entity within ten (10) days from the date of request of the Covered Entity.

D. Mitigation. Business Associate shall have procedures in place designed to mitigate, to the extent practical, any harmful effect that is known or reasonably foreseeable to the Business Associate of a use, access or disclosure of PHI by Business Associate in violation of the requirements of this Addendum, and Business Associate shall report its mitigation activity to the Covered Entity upon Covered Entity's request.

E. Notification of Breach, Suspected Breach, Loss, or Potential Loss of Confidential data or PHI.

i. During the term of this Addendum, the Business Associate shall notify the Covered Entity within three (3) days by telephone call plus e-mail, web form or fax upon the Discovery of any Breach by Business Associate of security of PHI or Suspected Breach of security of PHI (where the use or disclosure is not provided for and permitted by this Addendum) of which it becomes aware. In the event of any suspected Security Incident affecting Electronic PHI, unauthorized use or disclosure, loss, or potential loss of PHI as a result of Business Associate's violation of the Agreement and this Addendum, or potential loss of confidential data affecting the Agreement and this Addendum, the Business Associate shall notify the Covered Entity within three (3) days by telephone call plus e-mail, web form or fax.

ii. The Business Associate shall promptly investigate such Security Incident(s), Breach, Suspected Breach, or unauthorized use or disclosure of PHI or confidential data. Within ten (10) days 48 hours of the discovery of a Breach of Unsecured PHI by Business Associate, the Business Associate shall notify the Covered Entity's contract manager, and the Office of Technology Service Desk of:

a. What data elements were involved and the extent of the data involved in the Breach;

b. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data;

c. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

d. A description of the probable causes of the improper use or disclosure; and,

e. Whether any federal or state laws requiring individual notifications of Breaches are triggered. Covered Entity will coordinate with Business Associate to determine additional specific actions that will be required of the Business Associate or Covered Entity for mitigation of the Breach, suspected breach, or unauthorized use or disclosure of PHI, which may

include, but is not limited to, Covered Entity's notification to the individual, the media, HHS, or other authorities, as well as any other related notice requirements.

iii. Further, the Business Associate shall:

a. Conduct and document a risk assessment by investigating without unreasonable delay and in no case later than twenty (20) calendar days of Discovery of the Breach designed to determine the following:

1. Whether there has been an impermissible use, acquisition, access or disclosure of PHI under the HIPAA Privacy Rule;
2. Whether an impermissible use or disclosure compromises the security or privacy of the PHI by posing a significant risk of financial, reputational or other harm to the Client/Patient; and,
3. Whether the incident falls under one of the Breach exceptions contained in Section 13400(1)(B).

b. Provide completed risk assessment and investigation documentation to Covered Entity's Office of Compliance within twenty-five (25) calendar days of discovery of the potential breach with decision whether a Breach has occurred:

- i. If a Breach has not occurred, notification to Client/Patient(s) is not required.
- ii. If a Breach has occurred, and notification to the Client/Patient(s) is required, then Business Associate must provide Covered Entity with affected Client/Patient names and contact information (if known) so the Covered Entity can provide notification.

c. Make available to Covered Entity and governing State and Federal agencies in a reasonable time and manner designated by Covered Entity or governing State and Federal agencies, any policies, procedures, internal practices and records of Business Associate relating to a Breach or potential Breach for the purposes of audit or should the Covered Entity reserve the right to conduct its own investigation and analysis.

iv. All associated costs shall be borne by the Business Associate. This may include, but not be limited to costs associated with notifying the individuals or entities who are required by law to be notified as a result of a Breach of Unsecured PHI that is caused by Business Associate's violation of this Addendum. Depending on the nature and scope of such Breach of Unsecured PHI, Covered Entity's remedies may include, among other things, providing information to affected individuals on obtaining credit reports and notification to applicable credit card companies, notification to the local office of the secret

service, and or affected users and other applicable parties, utilization of a call center and the offering of credit monitoring services on a selected basis. Business Associate agrees that the Covered Entity shall be held harmless in the event of such a Breach and Business Associate accepts fully the legal and financial responsibility associated with mitigating any harmful effects that may or have been caused, including but not limited to the Business Associate and Covered Entity's required actions pursuant to HIPAA and HITECH as defined herein. Business Associate agrees that it is subject to shall comply with all HIPAA regulations in effect at the time of this Addendum and as shall be amended under HIPAA from time to time, and any and all reporting requirements required by HIPAA at the time of this Addendum and as shall be amended, under HIPAA, from time to time, as well as ensuring compliance with the Rhode Island Confidentiality of Health Care Information Act, Rhode Island General Laws, Sections 5-37.3 et seq., all only as are applicable to Business Associate in the performance of its obligations under the Agreement.

v. Assistance in Litigation or Administrative Proceedings. The Business Associate shall make itself and any subcontractors, employees or agents assisting the Business Associate in the performance of its obligations under the Agreement and/or this Addendum, available to the Covered Entity at no cost to the Covered Entity to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Covered Entity, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy which involves inaction or actions by the Business Associate, except where Business Associate or its subcontractor, employee or agent is a named as an adverse party.

F. Access to Protected Health Information. Business Associate shall make the PHI maintained by Business Associate or its agents or subcontractors available in Designated Record Sets to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act. Business Associate agrees to provide access to Protected Health Information, at the request of Covered Entity, in the time and manner designated, in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under 45 CFR 164.524. Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of the Covered Entity, available to the Secretary of the United States Dept. of Health and Human Services, in a time and manner specified by the Covered Entity or designated by the Secretary, for purposes of the Secretary determining the Covered Entity's compliance with the Privacy Rule.

G. Amendment of PHI. Within ten (10) days of receipt of a request from Covered Entity for an amendment of the PHI or a record about an individual maintained by Business Associate in a Designated Record Set, Business Associate or its agents or subcontractors shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526. Business Associate agrees to

make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 at the request of Covered Entity or an Individual, and in the time and manner specified by the Covered Entity.

H. Access to Records. Business Associate shall make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use, access and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, and/or to the Secretary for the U.S. Department of Health and Human Services, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rules and patient confidentiality regulations, consistent with 45 CFR 164.504. The respective rights and obligations of Business Associate under this section of this Addendum shall survive the termination of the Agreement.

I. Individual's Right to Access, Amend and Accounting of Disclosure(s). The Business Associate shall make available to the specific Individual to whom it applies any PHI; make such PHI available for amendment; and make available the PHI required to provide an accounting of disclosures, all to the extent required by 45 CFR §§ 164.524, 164.526, and 164.528 respectively. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. Business Associate agrees to provide to the Covered Entity or an Individual, in a time and manner specified by the Covered Entity, information collected in accordance with the Agreement, to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528 and the HITECH Act.

J. Security. The Business Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, the compliance with 74 FR 19006, "Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under Section 13402 of Title XIII" is required. If Business Associate chooses not to adopt such methodologies as defined in 74 FR 19006 based on its Security Risk Analysis, Business Associate shall document such rationale and submit it to the Covered Entity.

K. Duties at Termination. Upon termination of the Agreement and/or this Addendum for any reason, Business Associate shall return all Protected Health Information, in whatever form, required to be retained and return or destroy all other Protected Health Information received from the Covered Entity, or created or received by the Business Associate or its subcontractors, employees or agents on behalf of the Covered Entity. In the event the Business Associate determines that returning the Protected Health Information is not feasible (such as in the event that the retention of Protected Health Information is required for archival purposes to evidence Business Associate's services under the Agreement), the Business Associate may retain such information and shall, upon Covered Entity's request, provide the Covered Entity with written notification of the conditions that make return not feasible. The Covered Entity shall be the final

authority in determining whether the return of PHI is not feasible. However, the Covered Entity shall not unreasonably withhold its consent from Business Associate as to the feasibility of the return of PHI. Business Associate further agrees to extend any and all protections, limitations, and restrictions contained in the Agreement and/or this Addendum, to any Protected Health Information retained by Business Associate or its subcontractors, employees or agents after the termination of the Agreement and/or this Addendum. These protections, limitations and restriction shall also apply to all agents and subcontractors of Business Associate. The Business Associate shall limit any further use, access or disclosures to the purposes that make the return or destruction of the Protected Health Information infeasible. This shall also apply to all agents and subcontractors of Business Associate. The duty of the Business Associate and its agents and subcontractors to assist the Covered Entity with any HIPAA-required accounting of disclosures survives the termination of the Agreement and this Addendum.

L. Termination for Cause. Covered Entity may terminate the Agreement if at any time it determines that the Business Associate has violated a material term of the Agreement or this Addendum. Covered Entity may, at its sole discretion, allow Business Associate a reasonable period of time to cure the violation before termination.

M. Breach Pattern or Practice by Covered Entity. Pursuant to 42 U.S.C. Section 17934(b), if the Business Associate knows of a pattern of activity or practice of the Covered Entity that constitutes a material breach or violation of the Covered Entity's obligations under this Addendum, the Business Associate must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, the Business Associate must terminate the Addendum if feasible, or if termination is not feasible, report the problem to the Secretary of United States Department of Health and Human Services.

N. Judicial or Administrative Proceedings. The Covered Entity may terminate this Addendum if Business Associate is found guilty of a criminal violation of HIPAA. The Covered Entity may terminate this Addendum if a finding or stipulation is made in any administrative or civil proceeding in which the Business Associate is a party or has been joined that the Business Associate has violated any standard or requirement of HIPAA, HITECH or other security or privacy laws.

O. Subcontractors and Agents. The Business Associate will require any of its subcontractors and agents, to which the Business Associate is permitted by the Agreement or this Addendum or in writing by the Covered Entity to disclose the Covered Entity's Protected Health Information and/or Electronic Protected Health Information, to provide reasonable assurance that such subcontractor or agent will comply with the same privacy and security safeguard obligations with respect to the Covered Entity's Protected Health Information and/or Electronic Protected Health Information that are applicable to the Business Associate under this Addendum.

P. Designation of Compliance Official and Contact Individual. The Business Associate shall designate a compliance official who shall be responsible for the development and implementation of policies and procedures required of Business Associate under this Addendum. The Business Associate shall designate a contact individual or office for receiving complaints and shall provide documentation of such designation to the Covered Entity. The contact individual or office must be able to provide information about matters relating to Breaches of Unsecured PHI hereunder.

### **3. Specific Use and Disclosure Provisions.**

A. Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate as provided in 45 C.F.R. § 164.504(e)(4).

B. Business Associate may disclose PHI for the proper management and administration of the Business Associate as provided in 45 C.F.R. § 164.504(e)(4), or as Required by Law.

C. Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 CFR 164.504(e)(2)(i)(B).

D. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 42 CFR 164.502(j)(1).

### **4. Obligations of Covered Entity.**

A. Covered Entity shall notify Business Associate in writing of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use, access or disclosure of Protected Health Information.

B. Covered Entity shall notify Business Associate in writing of any changes in, or revocation of, permission by an individual to use, access or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use, access or disclosure of Protected Health Information.

C. Covered Entity shall notify Business Associate in writing of any restriction to the use, access or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use, access or disclosure of Protected Health Information.

D. Covered Entity shall complete the following in the event that the Covered Entity has determined that Business Associate has a breach:

i. Determine appropriate method of notification to the Client/Patient(s) regarding a breach as outlined under Section 13402(e) of the HITECH Act.

ii. Send notification to the Client/Patient(s) without unreasonable delay but in no case later than sixty (60) days of discovery of the breach with at least the minimal required elements as follows:

a. A brief description of what happened, including the date of the Breach and the date of discovery;

b. A description of the types of unsecured PHI involved in the Breach (such as name, date of birth, home address, Social Security number, medical insurance, etc.);

c. The steps Client/Patient(s) should take to protect themselves from potential harm resulting from the breach.

iii. Determine if notice is required to Secretary of the United States Department of Health and Human Services.

iv. Submit breach information to the Secretary of the U.S. Department of Health and Human Services within the required timeframe, in accordance with 45 CFR 164.408(b).

## **5. General Provisions.**

A. Remedies. Business Associate agrees that Covered Entity shall be entitled to seek immediate injunctive relief as well as to exercise all other rights and remedies which Covered Entity may have at law or in equity in the event of an unauthorized use, access or disclosure of Protected Health Information by Business Associate or any agent or subcontractor of Business Associate that received Protected Health Information from Business Associate.

B. Ownership. As between the parties, the Protected Health Information shall be and remain the property of the Covered Entity. Business Associate agrees that it acquires no title or rights to the Protected Health Information other than specifically set forth in this Addendum or the Agreement.

C. Regulatory References. A reference in this Addendum to a section in the HIPAA Privacy and Security Rules and patient confidentiality regulations means the section as in effect or as amended.

D. Amendment. The parties agree to take such action as is necessary to amend this Addendum from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HIPAA Privacy and Security Rules and the Health Insurance Portability and Accountability Act and patient confidentiality regulations.

E. Interpretation. Any ambiguity in this Addendum shall be resolved to permit Covered Entity and Business Associate to comply with the Privacy and Security Rules and patient confidentiality regulations.

F. Secondary PHI. Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an Individual must be held confidential and, as between the parties, is also the property of Covered Entity.

G. Electronic Transmission. Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an Individual must not be transmitted to another party by electronic or other means for additional uses not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Covered Entity except as otherwise permitted herein.

H. No Sales. Reports or data containing the PHI may not be sold without Covered Entity's or the affected Individual's written consent.

I. No Third-Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, benefits, remedies, obligations or liabilities whatsoever, whether in contract, statute, tort (such as negligence), or otherwise, and no person shall be deemed a third-party beneficiary under or by reason of this Addendum.

J. This Addendum constitutes the entire Business Associate Agreement Addendum and supersedes all prior Business Associate Agreement Addenda and understandings, both written and oral, among the Parties with respect to the subject matter of this Addendum.

K. This Addendum shall be binding upon, inure to the benefit of, and be enforceable by and against the Parties and their respective heirs, personal representatives, successors, and assigns. Neither this Agreement nor any of the rights, interests or obligations under this Addendum shall be transferred or assigned by the Business Associate without the prior written consent of the Covered Entity.

L. With respect to any provision of this Addendum finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Addendum cannot be reformed, such provision shall be deemed severed from this Agreement, but every other provision of this Addendum shall remain in full force and effect. This Addendum shall be governed by, and construed in accordance with, the laws of the State of Rhode Island.

M. All representations, covenants, and agreements in this Addendum that by their nature should survive the termination of this Addendum shall survive the execution, delivery, and performance of this Addendum.

N. Each Party shall execute, acknowledge or verify, and deliver any and all documents that may, from time to time, be reasonably requested by the other Party to carry out the purpose and intent of this Addendum.

## **6. Acknowledgment.**

A. Notwithstanding any other requirement set out in this Addendum, the Contractor acknowledges and agrees that the HITECH Act and its implementing regulations impose new requirements with respect to privacy, security and breach notification and contemplates that such requirements shall be implemented by regulations to be adopted by the Department of Health and Human Services. The HITECH requirements, regulations and provisions are hereby incorporated by reference into this Addendum as if set forth in this Addendum in their entirety. Notwithstanding anything to the contrary or any provision that may be more restrictive within this Addendum, all requirements and provisions of HITECH, and its implementing regulations currently in effect and promulgated and/or implemented after the date of this Addendum, are automatically

effective and incorporated herein. Where this Addendum requires stricter guidelines, the stricter guidelines must be adhered to.

**B. By signing this Addendum, the Business Associate agrees that this Addendum shall binding during the Interim Final Rules and until such time as Final Rules are promulgated and a new Business Associate Agreement Addendum is signed based on the Final Rules. The Business Associate agrees that it shall sign a new mutually agreeable Addendum based on the new Final Rules when presented by the Rhode Island Executive Office of Health and Human Services.**

C. The undersigned affirms that he/she is a duly authorized representative of the Business Associate for which he/she is signing and has the authority to execute this Addendum on behalf of the Business Associate.

Acknowledged and agreed to by:

Office of the Governor  
Division of the Rhode Island  
Health Benefits Exchange

[Legal Name of Business Associate]

\_\_\_\_\_  
AUTHORIZED AGENT/SIGNATURE

\_\_\_\_\_  
AUTHORIZED AGENT/SIGNATURE

TITLE: \_\_\_\_\_

TITLE: \_\_\_\_\_

\_\_\_\_\_  
PRINT NAME

\_\_\_\_\_  
PRINT NAME

\_\_\_\_\_  
DATE

\_\_\_\_\_  
DATE