BUSINESS ASSOCIATE AGREEMENT STANDARD TERMS AND CONDITIONS
BY AND BETWEEN
COMMUNITY RESOURCE INITIATIVE
AND
[VENDOR]

I. GENERAL PROVISIONS

Section 1. Community Resource Initiative (CRI) has entered a Business Associate Agreement (BAA) with Department of Public Health of Massachusetts (Department). Under the terms of the BAA Department is a Covered Entity under the Health Insurance Portability and Accountability Act (HIPAA) and CRI is a Business Associate of Department. As a Business Associate CRI is required to enter into a contract with each of its subcontractors who provide services on behalf of CRI related to CRI's provision of services to Department.

Section 2. CRI and ___(Vendor) have entered into an agreement (Agreement) under which Vendor is a subcontractor who provides services on behalf of CRI related to CRI's provision of services to Department. Vendor acknowledges that Vendor, in its performance of its duties under the Agreement will come into contact with Protected Health Information related to the Department which is the subject of the BAA between CRI and Department, and hereby agrees to be bound by the terms of this Contract (this Contract). The parties agree that terms of this Contract are based off the BAA entered by and between CRI and Department, and Department is the intended Covered Entity. Any reference to Covered Entity shall mean Department.

Section 3. Contract Terms and Conditions. The terms of this Contract are intended to protect the privacy and security of all Personal Data, including Protected Health Information, that the Vendor may receive from and/or create on behalf of CRI in the performance of its duties and responsibilities under the Agreement, and to ensure that the CRI complies with its obligations as a BA of Department.

II. DEFINITIONS FOR USE IN THIS CONTRACT

All terms used, but not otherwise defined herein shall be construed in a manner consistent with the HIPAA Privacy and Security Rules, The Fair Information Practices Act, and other applicable state or federal privacy or confidentiality laws.

"Breach" means the acquisition, access, use, or disclosure of protected health information in a manner not permitted, under HIPAA or M.G.L. c. 93 H which compromises the security or privacy of the PHI.

"Business Associate" means a person or entity, who, on behalf of a covered component of CRI, and other than in the capacity of a workforce member, performs or assists in the performance of a function or activity that involves the use or disclosure of protected health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services, where the provision of the service involves the use or disclosure of protected health information.

"Data Subject" means an individual to whom Personal Data or Protected Health Information refers.

"Electronic Media" means:

Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Faxes sent directly from one fax machine to another, person- to-person telephone calls, video teleconferencing, and messages left on voice-mail are not considered transmission media. However, any faxes sent from a computer, including those made by a fax-back system, are considered transmission media.

"Electronic Protected Health Information" (EPHI) means PHI that is created, accessed, stored, or transmitted by electronic media.

"The Health Insurance Portability and Accountability Act" (HIPAA) means Public Law 104-191.

"The HITECH Act" means Title XII of the American Recovery and Reinvestment Act of 2009, specifically the provision s of Subtitle D - Privacy, which shall hereinafter be included under references to HIPAA.

"Personal Data" (PD) means any information in any medium concerning an individual, which because of name, identifying number, mark or description can be associated with a particular individual. Protected Health Information and Electronic Protected Health Information as defined herein, constitute subsets of Personal Data.

"Privacy Rule" means the privacy regulations set forth in 45 C.F.R. Parts 160 and 164 and as amended.

"Protected Health Information" (PHI) means information in any form or medium that relates to the past, present or future, physical or mental 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 that identifies the individual or with respect to which there is a reasonable basis to believe can be used to identify the individual, that the Vendor receives, creates or uses under the Agreement. The terms "Protected Health Information" and "PHI" apply to the original data and to any data derived or extracted from the original data. PHI includes EPHI and is a subset of Personal Data.

"Required By Law" means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law.

"Secretary" means the Secretary for the Office of Health and Human Services or her/his designee.

"Security Rule" means the Security standards for the protection of EPHI as set forth at 45 C.F.R. Parts 160, 162 and 164 and as amended.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

III. OBLIGATIONS OF THE VENDOR

Section 1. Compliance with State and Federal Law. The Vendor acknowledges that in the performance of the Agreement, it may receive PHI. The Vendor acknowledges that by accepting the PHI it becomes a "holder" within the meaning of M.G.L. c. 66A and will comply with the requirements of that law in addition to HIPAA and all other applicable state or federal laws governing the privacy or security of any PHI received or created under the Agreement.

Section 2. Ownership of PHI. The Vendor shall at all times recognize CRI as sole owner of the PHI as between CRI and Vendor. As owner of the PHI, CRI shall at all times have complete control over the use, disclosure and disposition of the PHI include, if relevant, editorial control over the output.

Section 3. Agreement of Third Parties. The Vendor shall not engage a subcontractor or agent that will receive PHI originating from CRI or create or receive PHI on behalf of CRI without prior authorization from CRI. If CRI authorizes the Vendor in advance to engage such a subcontractor or an agent, CRI shall obtain and maintain a written agreement with each agent or subcontractor. The agreement shall provide that such agent or subcontractor agrees to be bound by the same restrictions, terms and conditions that apply to the Vendor pursuant to the Agreement with respect to such PHI, including but not limited to implementing reasonable and appropriate safeguards to protect the information. All provisions of this Contract apply to all such PHI, whether in the possession of the Vendor or any agent or subcontractor. The Vendor is responsible for ensuring each agent's and subcontractor's compliance with all applicable provisions of this Contract. Upon request, the Vendor shall provide CRI with a copy of the written terms between the Vendor and the subcontractor or agent.

Section 4. Compliance with Use and Disclosure Provisions. Vendor agrees to comply with the use and disclosure provisions of HIPAA as established in 45 CFR §164.502(e)(2) and the requirements of §164.504(e) shall apply to Vendor in the same way they apply to CRI.

Section 5. Security. Appropriate Safeguards. 45 CFR §§164.308, 164.310, 164.312 and 164.316 shall apply to the Vendor. Vendor agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI. Such safeguards shall meet, at a minimum, the standards as set forth in the Privacy and Security Rules, and Department standards. Appropriate safeguards shall include, at a minimum:

- Protecting the physical and electronic security of the PHI, including any data created, accessed, stored, or transmitted by electronic media.
- Compliance with applicable provisions of Executive Order 504.
- Not removing any data from Commonwealth premises, unless authorized under the Agreement and notifying CRI prior to such removal.
- Taking steps to prevent unauthorized access to the PHI, including preventing unauthorized access through the use of individual user accounts which are password protected and can be audited.

- Providing appropriate training in the privacy and security policies and procedures applicable to PHI for each of its employees, agents, or subcontractors who will have access to CRI's PHI as set forth

- Requiring each of its employees, agents, or subcontractors having any involvement with the PHI to comply with applicable laws and regulations relating to confidentiality and privacy of the PHI as well as the security of EPHI.

- To the extent that the Vendor's employees physically work on site at CRI, they shall be. subject to CRI's and the Department's Confidentiality and Security Policies and Procedures.

- Laptop security. When a laptop maintaining PHI is not in use, the laptop must be secured as encrypted files in an encrypted volume on the hard drive (Example: PGP Disk File and Disk Encryption). Laptops should not be left unattended and must be stored securely in locked cabinets or rooms. Portable electronic media used to maintain PHI must include encryption functionality, and must be stored in locked cabinets or rooms.

USB Thumb Drives must have password or biometric protection to provide for encrypted file security. The encryption must be enabled whenever the PHI is not being used. (Example: the Lexar Jumpdrive Secure)

PHI stored on a CD-Rom must be maintained in an encrypted file. (Example: WinZip 9 with 256 bit AES encryption)

- Unless otherwise authorized, under the terms of the Agreement, all copies of any CRI data stored on electronic storage media, including thumb drives, controlled by Vendor must, be destroyed upon termination of the Agreement. Data must be destroyed so that it cannot be recovered from the electronic storage media. Acceptable methods include the use of file wiping software implementing at a minimum DoD.5200.28-STD (7) disk wiping, and the degaussing of backup tapes. Electronic storage media such as floppy disks, CDs, and DVDs us d to store data must be made unusable by physical destruction.

- Upon request, the Vendor will furnish CRI with a description of the steps it has taken to prevent use or disclosure of the PHI not authorized by this Contract or the Agreement and agrees to allow authorized representatives of CRI access to premises where the PHI is kept for the purpose of inspecting security (physical and electronic) arrangements.

Section 6. Non-Secure Transmissions Prohibited. The Vendor agrees that it will not transmit the PHI over any unsecured network or over any wireless communication device without the prior written permission of the designated representative of CRI. Transmissions over the Internet must be limited to the secure transmission protocols and methods specified in the Agreement. The Vendor is expected to comply with NIST standards FIPS 140-2 when transmitting PHI over the Internet.

Section 7. Reporting of Breach or Security Incident. The Vendor shall notify the designated representative for CRI under the Agreement both orally and in writing within three (3) days following the discovery of any breach of PHI, including but not limited to any use or disclosure of unsecured PHI not

permitted under the Agreement or any security incident involving or potentially involving CRI's PHI.

Section 8. Responsibility for Breach Notification. The Vendor shall pay the full cost of breach notification for any notification required under HIPAA or M.G.L. c. 93 A, for any breach for which Vendor, its agents or employees is responsible or any breach that occurred through its information system(s), whether the notice is given by CRI or Vendor.

Section 9. Mitigation. The Vendor shall mitigate, to the extent practicable, any harmful effect that is known to the Vendor of its use or disclosure of PHI in violation of the Agreement or any security breach. The Vendor shall in consultation with CRI take measures that CRI deems appropriate to recover the PHI and prevent a future breach of the confidentiality and security of the PHI.

The Vendor shall report to the Covered Entity the results of all mitigation actions taken. Nothing in this Section will be deemed to waive any of CRI's or the Department's legal rights or remedies that arise from the Vendor's unauthorized use or disclosure of the PHI or security breach.

Section 10. Red Flags Rule. Where applicable, and at the direction of CRI, Vendor shall implement and maintain appropriate identity theft management programs in compliance with the federal Red Flags Rule.

Section 11. Notice of Request for Data. The Vendor agrees to notify CRI within three (3) days of the Vendor's receipt of any legal request, court order, or subpoena for PHI. To the; extent that CRI decides to assume responsibility for challenging, the validity of such requests, the Vendor agrees to cooperate fully with CRI in such challenge.

Section 12. Access to PHI.

A. The Vendor shall provide CRI with access to or copies of any PHI, which it maintains pursuant to the Agreement;

B. The Vendor shall also provide access directly to an individual's PHI, unless otherwise restricted by law, if the individual makes a request directly to the Vendor, as shall be necessary to meet its obligation under 45 C.F.R. § 164.524 and M.G.L. c. 66A.

C. Such access or copies shall be provided to CRI and/or Department or requesting representative or requesting within three (3) days of a request.

Section 13. Availability of PHI for Amendment. The Vendor shall allow an individual to make requests to amend his or her PHI that the Vendor maintains and for which the Vendor is the source. The Vendor shall also make any amendment(s) to PHI that it received from or created or received on behalf of CRI that CRI directs, in or for CRI to meet its obligations under 45 C.F.R. §
164.526 and M.G.L c.66A. All such amendments shall be made within eight (8) days of the request from CRI.

Section 14. Accounting of Disclosures. The Vendor shall document PHI disclosures and required information related to such disclosures, as is necessary for CRI to respond to an individual's request for accounting of disclosures of PHI under 45 C.F.R. § 164.528 and M.G.L. c. 66A. The Vendor

agrees to provide to CRI or the requesting individual, within ten (10) days of the request an accounting of disclosures of PHI. At a minimum, the Vendor will provide the following information i} the date of the disclosure, (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure. The Vendor agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section and to provide upon CRI's request, documentation of its method of tracking disclosures and a list of all accountings of disclosures provided under this Section.

Section 15. Access by Secretary to Records. The Vendor shall make available to CRI or the Secretary its internal practices, books, and records including policies and procedures relating to the use and disclosure of the PHI received from CRI, or created or received by the Vendor on behalf of CRI as well as policies and procedures relating to the confidentiality and security of the data. CRI or the Secretary shall determine the time and manner for making such material available for purposes of the Secretary determining CRI's compliance with the Privacy and Security Rules.

Section 16. Prohibition on the Sale of PHI or Electronic Health Records. The Vendor shall comply with 45 CFR § 164.502(a)(5), which relates to the prohibition on the sale of electronic health records and PHI.

IV. PERMITTED USES AND DISCLOSURES BY THE VENDOR

Section 1. Uses and Disclosures of PHI. The Vendor agrees to use or disclose PHI that it receives from or creates or receives on behalf of CRI only as specified in this Section IV or as required by law.

A. To Perform the Agreement. The Vendor may use or disclose PHI, or create PHI on behalf of CRI, as is necessary for the Vendor to administer or perform the functions, activities and services that are required to satisfy its obligations under the Agreement. This shall include providing the Secretary and CRI with full access to such PHI for purposes of auditing the performance of the Vendor under the Agreement and as CRI determines is otherwise necessary for: (1) providing treatment to individuals receiving services under the Agreement; (2) the payment for or reimbursement of those services; and/or (3) health care operations. Operations shall include reporting to CRI to fulfill state or federal reporting requirements. If the Vendor concludes that a client authorization is required for the release of PHI to CRI as required in this section, the Vendor agrees to timely secure client authorizations.

B. For Research or Publication. The Vendor agrees that it shall not conduct any research utilizing the PHI received from CRI or created or derived from the data received from and/or created under the Agreement for research purposes without application to and the written approval of CRI for the specific research. Further the Vendor agrees that it shall not utilize the PHI received from or created or derived from such data without the written approval of CRI for the specific publication. Vendor acknowledges that any approval for use of PHI as stated herein is required from Department and until Vendor is notified in writing by CRI of Department’s approval, if given, Vendor will not conduct any research or publication.

C. For Management and Administration. The Vendor may use PHI that it receives from and/or creates or receives on behalf of CRI for the proper management and, administration of the Vendor as provided for by 45 C.F.R. § 164.504(e)(4), provided that such use complies with the requirements of the Agreement, this Business Associate Agreement, and all other applicable state or federal privacy laws.

Section 2. Minimum Necessary. The Vendor agrees to take reasonable steps to limit the amount of PHI used and/or disclosed pursuant to Section 1 above to the minimum necessary to achieve the purpose of the use and disclosure.

V. OBLIGATIONS OF CRI

Section 1. Notice of Privacy Practices. CRI shall notify the Vendor of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect the Vendor's use or disclosure of PHI.

Section 2. Revocation of Permission to Use PHI. CRI shall notify the Vendor of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent that such changes may affect the Vendor's use or disclosure of PHI.

Section 3. Restriction to Use or Disclose PHI. CRI shall notify the Vendor of any restriction to the use or disclosure of PHI that CRI has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such changes may affect the Vendor’s use or disclosure of PHI.

Section 4. Notice of Changes and Restrictions. Covered Entity shall notify Vendor of any changes in, or revocation of, permission by an individual to use or disclose PHI, to the extent such changes affect Vendor's permitted or required uses and disclosures. Such notification shall include any restriction that Covered Entity has agreed to in accordance with 45 CFR § 164.522. If Vendor receives a request to restrict the disclosure of PHI directly from an Individual, Vendor shall notify CRI of such request and CRI shall be responsible for making the determination, in accordance with the Privacy Rule, as to whether Vendor shall comply with the Individual's request.

VI. TERMINATION OR COMPLETION OF AGREEMENT WITH THE VENDOR

Section 1. Termination Upon Breach of Confidentiality or Security Provisions Applicable to PHI. CRI may terminate the Agreement and this Contract immediately upon written notice, if CRI determines in its sole discretion, that the Vendor has materially breached any of its obligations regarding PHI. Prior to terminating the Agreement, CRI, in its sole discretion, may provide an opportunity for the Vendor to cure the breach or end the violations. If such an opportunity is provided, but cure is not feasible, or the Vendor fails to cure the breach or end the violations within a time period set by CRI, CRI may terminate the Agreement immediately upon written notice.

Section 2. Termination by Expiration or Termination of the Agreement. This Contract will terminate concurrently upon the termination or expiration of the Agreement.

Section 3. Termination is Not Feasible. In the event that termination of the Agreement is not feasible, in CRI's sole discretion, the Vendor hereby acknowledges that CRI will have the

right to report this breach to the Secretary, notwithstanding any other provisions of this Agreement to the contrary.

Section 4. Effect of Termination or Completion.

A. The Vendor agrees that within ten (10) days of the termination or completion of the Agreement, it will return or destroy, at CRI's direction and according to standards approved by CRI, any and all PHI that it maintains in any form, including PHI that is in the possession of its subcontractors or agents and will retain no copies of the PHI.

B. Notwithstanding the foregoing, to the extent that CRI agrees that if it is not feasible to return or destroy such PHI, all protections pertaining to any PHI covered by the Agreement shall remain in force and the Vendor will limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Vendor maintains such PHI.

Section 4. Transition Assistance. Following the termination of this Contract for any reason, the Vendor agrees to provide transition services for the benefit of CRI, including the continued provision of its services required under the Agreement until notified by CRI that an alternative provider of services is able to take over the provision of such services and the transfer of PHI and other data held by the Vendor related to its services under the Agreement.

Section 1. Regulatory References. A reference in this Contract or the Agreement to a section of the Privacy or Security Rule means the section as in effect or as amended.

Section 2. Survival. The obligations of the Vendor under Part VI of this Contract shall survive the termination of this Contract.

Section 3. Amendment. The Vendor and CRI agree to negotiate to amend the Contract to the extent necessary to allow either party to comply with amendments to the Privacy or Security Rules or the Standards for Electronic Transactions.

Section 4. Remedies. Nothing in this Agreement shall be construed to waive or limit any of CRI's or Department’s legal rights or remedies that may arise from the Vendor's unauthorized disclosure of PHI or security breach. CRI's exercise or non-exercise of any authority under the Agreement including, for example, any rights of inspection or approval of privacy or security practices or approval of subcontractors, shall not relieve the Vendor of any obligations as set forth herein nor be construed as a waiver of any of the Vendor's obligations, or as an acceptance of any unsatisfactory practices, or privacy or security failures by the Vendor. Department is third party beneficiary for purposes of enforcing its legal rights under or related to this Contract.

Section 5. Interpretation. Any ambiguity in the Agreement shall be resolved to permit CRI to comply with HIPAA's Privacy or Security Rules, M.G.L. c. 66A, M.G.L. c. 93 H, and any other law pertaining to the privacy or security of PHI.

The parties hereto have caused their duly authorized representatives to execute this Contract.