

## Business Associate Agreement

This Agreement, effective \_\_\_\_\_ is entered into by and between the covered entity, **ABC** (hereafter known as **ABC**) and the business associate, **Vendor Name** (hereafter known as **Business Associate**). **Vendor will provide a private engagement network platform to connect, engage and influence alumni.**

This contract is in accordance with **ABC** obligations under:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the applicable requirements of HIPAA's implementing regulations issued by the U.S. Department of Health and Human Services, Title 45 of the Code of Federal Regulations ("C.F.R.") Parts 160-164 ("HIPAA Regulations");
- The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as incorporated in the American Recovery and Reinvestment Act of 2009, Public Law 111-005;
- The Genetic Information Nondiscrimination Act (the "GINA")

Each may be amended from time to time, to ensure the integrity and confidentiality of individually identifiable personal and health information that a business associate may create for, or receive from a covered entity. **Business Associate** acknowledges and agrees that **Business Associate** is obligated by law to meet the applicable provisions of HIPAA and the HITECH Act and regulations issued thereunder.

### **A. Definitions.**

1. **"Breach"** shall mean the illegal or unauthorized acquisition, access, use, or disclosure of PHI which compromises the security, confidentiality, privacy, or integrity of such information pursuant to the HITECH Act § 13400, any regulations issued there under, or as amended by law.
2. **"Business Associate"** means an individual or entity who or which performs a function or activity on behalf of, or provides a service to ABC that involves the creation, use or disclosure of PHI. Shall have the meaning given to such term under the HIPAA Privacy Rule, the HIPAA Security Rule, and the HITECH Act, but not limited to, Section 13400 and Section 13401 of the HITECH Act, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.
3. **"Covered Entity"** means a health plan, health care clearinghouse or a health care provider who transmits any health information in electronic form in connection with a

transaction covered under the HIPAA Regulations. Covered Entity shall have the meaning given to such term under the HIPAA Privacy Rule and the HIPAA Security Rule, including but not limited to, 45 C.F.R. Section 160.103. **ABC** is a Covered Entity.

4. **"Designated Record Set"** means a group of records maintained by or for **ABC** comprising the electronic health records, enrollment, payment, claims adjudication and case or medical management record systems maintained by or for **ABC**, or used in whole or in part, by or for **ABC**. For purposes of this definition, the term "record" includes any item, collection, or grouping of information that contains PHI and is maintained, collected, used, or disseminated by or for **ABC**.
5. **"E PHI"** means PHI maintained or transmitted in electronic form.
6. **"Limited Data Set"** shall mean PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. (See 45 C.F.R. § 164.514(e)(2)).
7. **"Personal and Protected Health Information"** ("PHI") means either medical information or individually identifiable information in electronic, physical or oral form. Medical information is any information in possession of, or derived from, a physician or other provider of health care or a health care service plan regarding an individual's medical history, mental or physical condition, or treatment. Individually identifiable information is that which contains any element of personal identifying information sufficient to allow identification of the individual, such as the individual's name, address, electronic mail address, telephone number, or social security number, or other information, alone or in combination with other publicly available information, which reveals the individual's identity. PHI shall have the meaning given to such term under the HIPAA Privacy Rule and the GINA, including, but not limited to, 45 C.F.R. Section 164.501. PHI includes Electronic Protected Health Information (E PHI) (45 C.F.R. Sections 160.103, 164.501).
8. **"Privacy Official"** means the **ABC** individual and such individual's designees who are responsible for the development and implementation of **ABC**' policies and procedures regarding privacy and confidentiality of PHI.
9. **"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 that is created, received maintained or transmitted by or on behalf of **ABC**. (See 45 C.F.R. §164.304).
10. **"Required by law"** has the same meaning as the term "required by law" in 45 C.F.R.

§164.103.

11. **"Offshore Contractor"** refers to a contractor who is in a country that is not one of the fifty United States or one of the United States Territories (American Samoa, Guam, Northern Marianas, Puerto Rico, and Virgin Islands).
12. **"Subcontractor"** Subcontractor shall have the meaning given to such term under the HIPAA Privacy Rule, the HIPAA Security Rule, and the HITECH Act, including but not limited to, 42 U.S.C. Section 17938 and 45 C.F.R. Section 160.103.
13. **"Unsecured PHI"** means PHI that is not secured in accordance with guidance issued by the U.S. Department of Health and Human Services under the HITECH Act including, but not limited to, 42 U.S.C. Section 17932(h) and applicable regulations issued thereunder.

**B. Privacy and Security of PHI.**

1. **Permitted Uses and Disclosures.** **Business Associate** is permitted or required to use or disclose PHI it creates for or receives, maintains or transmits from **ABC** only as follows:
  - a. **Functions and Activities on ABC' Behalf.** **Business Associate** is permitted to use and disclose the minimum necessary PHI it creates for or receives from **ABC** in order to provide those services set forth in the Agreement, provided that no such use or disclosure would violate HIPAA Regulations or the HITECH Act and applicable regulations issued thereunder, if **ABC** made the use or disclosure.
  - b. **Vendor Operations.** **Business Associate** may use and disclose the minimum necessary PHI it creates, transmits or maintains for or receives, from **ABC** as necessary in order to perform **Business Associate's** obligations under the Agreement, **Business Associate's** proper management and administration, or to carry out **Business Associate's** legal responsibilities.
2. **Prohibition on Unauthorized Use or Disclosure.** **Business Associate** shall neither use nor disclose PHI it creates for or receives, maintains or transmits from **ABC**, except as permitted or required by this Agreement, as required by law, or as otherwise permitted in writing by **ABC**. **Business Associate** acknowledges that **Business Associate** may be liable for violating any of the requirements of this Agreement relating to the use or disclosure of PHI or any privacy-related requirements of the HITECH Act and regulations issued thereunder.
3. **Compliance with ABC' Confidentiality/Privacy Policies.** **Business Associate** shall comply with **ABC' Confidentiality/Privacy Policies**, including the Notice of Privacy

Practices which is distributed by **ABC. Business Associate** shall request a copy of all policies and notices that it does not already possess in order to review the requirements and comply with those requirements.

4. **Compliance with Laws; Regulatory Amendments.** **Business Associate** shall comply with all applicable state and federal privacy and security laws pursuant to HIPAA, HIPAA Regulations, the HITECH Act and any regulations promulgated thereunder. Any regulations or amendments to applicable privacy and security laws shall be automatically included in this Agreement such that this Agreement remains in compliance with such regulations or amendments. Any future state privacy and security laws shall be automatically included in this Agreement such that this agreement remains in compliance with such regulations or amendments.
5. **Information Safeguards.** **Business Associate** shall develop, implement, maintain and use appropriate administrative, technical and physical safeguards, in compliance with applicable state and federal laws, to preserve the integrity, confidentiality, and availability of PHI, and to prevent unauthorized disclosures of PHI created or received for or from **ABC** as required by 45 C.F.R. Part 164, Subpart C (Security Rule) and the HITECH Act and applicable regulations issued thereunder. **Business Associate** shall document and keep such safeguards current and shall develop and implement policies and procedures to meet the Security Rule documentation requirements of the HITECH Act and shall, upon **ABC'** request, either verbally or in writing, provide **ABC** with a copy of its policies and procedures related to such safeguards. **Business Associate** shall also provide reasonable description of the practices and processes that are in place to support the policies, procedures, and requirements.
6. **Subcontractors and Agents.** **Business Associate** shall require any of its subcontractors and agents to which **Business Associate** is permitted by this Agreement or in writing by **ABC** to disclose PHI, to sign a further Business Associate Agreement and to provide reasonable assurance evidenced by written contract, that such subcontractor or agent shall comply with the same privacy and security safeguard obligations with respect to PHI that are applicable to **Business Associate** under this Agreement, including, but not limited to: (i) holding such PHI in confidence and using or further disclosing it only for the purpose for which **Business Associate** disclosed it to the agent, subcontractor or other third party or as required by law; (ii) providing notification to **Business Associate** (who shall in turn notify, within two calendar days, **ABC**) of any instance of which the agent, subcontractor or other third party becomes aware in which the confidentiality of such PHI was Breached; and (iii) transmitting or sharing any PHI to any recipient Offshore without first obtaining written consent from **ABC** as to such Offshore transmission. Furthermore, such agents and subcontractors shall agree to notify **Business Associate** within two calendar days of any compromise

of PHI, and **Business Associate** will, in turn, notify **ABC**.

7. **Minimum Necessary and Limited Data Set.** **Business Associate's** use, disclosure or request of PHI shall utilize a Limited Data Set whenever possible. Otherwise, **Business Associate** shall, in its performance of the functions, activities, services, and operations specified in Section B.1 above, make reasonable efforts to use, to disclose, and to request only the minimum amount of PHI reasonably necessary to accomplish the intended purpose of the use, disclosure or request, except that **Business Associate** shall not be obligated to comply with the minimum necessary limitations with respect to those exceptions specified in 45 C.F.R. § 164.502(b) (2). **Business Associate** shall comply with the requirements governing the minimum necessary use and disclosure of PHI set forth in the HITECH Act § 13405(b) and any applicable regulations or other guidance issued thereunder.
8. **Transmission of Data Offshore.** **Business Associate** is not authorized or permitted to transmit or share any PHI to any recipient offshore without first obtaining written consent from **ABC** as to such offshore transmission. Verbal consent shall not suffice as permission to transmit or share any PHI with any recipient offshore. In support of such a request to **ABC**, **Business Associate** shall provide written evidence of offshore recipient's privacy and security policies, practices and safeguards. The **Business Associate** shall ensure that such offshore employees and contractors who access or utilize any PHI shall have completed privacy training in accordance with the Privacy Rule, Security Rule, HITECH Act and applicable state law. **ABC** may request copies of training materials and verifications of attendance and competency of training. The obligations of this section are in addition to **Business Associate's** obligations under Section B.6, above.

**C. PHI Access, Amendment, Disclosure, and Disclosure and Breach Reporting.**

1. **Access.** **Business Associate** shall, upon **ABC's** reasonable request and within ten (10) business days of receipt of request, permit an individual (or the individual's personal representative) to inspect and obtain copies of any PHI about the individual which **Business Associate** created or received for or from **ABC** and that is in **Business Associate's** custody or control. **Business Associate** shall provide such information in an electronic format, if requested by the individual and as directed by **ABC**.
2. **Amendment.** **Vendor** shall, upon receipt of notice from **ABC**, promptly amend or permit **ABC** access to amend, any portion of an individual's PHI which **Business Associate** created or received for or from **ABC** and that is in **Business Associate's** custody or control.
3. **Disclosure Accounting.** Upon request, **Vendor** shall forward to **ABC** a report of

disclosures as required by 45 C.F.R. § 164.528, and as applicable, the HITECH Act § 13405(c) and any regulations issued thereunder.

4. **Disclosure Accounting Retention.** **Business Associate** shall maintain an accounting of such disclosures for six (6) years after the date of occurrence and not prior to the Privacy Rule compliance date (April 14, 2003).

**5. Disclosure and Breach Reporting.**

- a. **Legal or Authorized Disclosure Reporting.** Except as permitted by applicable law, **Business Associate** shall document each disclosure it makes of an individual's PHI to a third party. Such report shall include the affected individual's name, the person or entity to whom the PHI was disclosed, what was disclosed, why the information was disclosed, the date of such disclosure and any other information necessary for **ABC** to comply with relevant statutes and regulations. Such report shall be furnished to **ABC** within ten (10) calendar days of its request. In addition, where **Business Associate** is contacted directly by an individual based on information provided to the individual by **ABC**, and where so required by the HITECH Act and/or any accompanying regulations, **Business Associate** shall make such report available directly to the individual.
- b. **Breach Reporting.** **Business Associate** shall report to **ABC** any Breaches of PHI. **Business Associate** shall make such report to **ABC**' Privacy Official not more than two calendar days after **Business Associate** knows, or should reasonably have known, of such Breach. **Business Associate** shall cooperate with **ABC** in investigating such Breach, and in meeting **ABC**' obligations under the HITECH Act and any other security breach notification laws. **Business Associate** shall report all Breaches to **ABC** in writing (and in the format requested by **ABC**) and such reports shall, at a minimum:
  - i. Identify the nature of the Breach including the date of the Breach and the date of discovery of the Breach;
  - ii. Identify which elements of the PHI (e.g., full name, social security number, date of birth, etc.) were breached, or were part of the Breach;
  - iii. Identify who was responsible for the Breach and who received the PHI;
  - iv. Identify what corrective actions **Business Associate** took or will take to prevent further incidents of a Breach;
  - v. Identify what **Business Associate** did or will do to mitigate any deleterious effect

of the Breach;

- vi. Identify **Business Associate** contact information and procedures to enable **ABC** to obtain additional information if required; and
  - vii. Provide such other information, including a written report, as **ABC** may reasonably request.
  - viii. **Business Associate** shall reimburse **ABC** for all Breach notification costs arising out of or in connection with, any Breach, including but not limited to, postage and mailing fees and the provision of credit monitoring services for affected individuals.
- c. **Security Incident Reporting.** **Business Associate** shall report to **ABC'** Chief Privacy Official and Chief Security Official within two calendar days after **Business Associate** knows, or should reasonably have known, of such Security Incident, any Security Incident of which **Business Associate** becomes aware. In addition, **Business Associate** shall, upon **ABC'** request, report any attempted unauthorized access, use, disclosure, modification, or destruction of EPHI. If any such security incident resulted in a disclosure of PHI not permitted by this Agreement, **Business Associate** shall make a report in accordance with Section C.5(b), above. If **Business Associate** is aware of a pattern of activity or practice by its subcontractor that constitutes a breach or violation of the subcontractor's obligations under its Business Associates Agreement or obligations with **Business Associate**, **Business Associate** must take reasonable steps to cure the breach or end the violation and take further actions consistent with 45 C.F.R. § 164.504.
- d. **Obligations in the Event of an Improper Pattern of Activity or Practice.** In the event that either party becomes aware of a pattern of activity or practice of the other party that constitutes a material breach or violation of this Agreement, the party discovering such pattern of activity or practice must take reasonable steps to cause the other party to cure the breach or end the violation. If a cure is not effectuated within a reasonable time period specified by the party requesting the cure, such party shall terminate this Agreement, if feasible, or if not feasible, report the problem to the Secretary of the U.S. Department of Health and Human Services or its designee. (See 45 C.F.R. § 164.504(e)(1)(ii) and HITECH Act § 13404(b)).
6. **Inspection of Books and Records.** **Business Associate** shall make available for inspection its internal practices, books, and records (relating to its use and disclosure of the PHI it creates for, or receives from, **ABC**) to **ABC** and/or the U.S. Department of Health and Human Services to determine compliance with the HIPAA Regulations or the

**Business Associate's** compliance with this Agreement.

7. **Designated Record Set. Vendor** agrees that all PHI received by or created for **ABC** shall be included in an individual's Designated Record Set. **Vendor** shall maintain such Designated Record Set with respect to services provided to an individual under this Agreement, and shall allow such individual to access the Designated Record Set as provided in the HIPAA Regulations.
8. **Restriction Agreements and Confidential Communications. Business Associate** shall comply with any agreement that **ABC** makes that either; (i) restricts use or disclosure of PHI pursuant to 45 C.F.R. § 164.522(a); or (ii) requires confidential communication about PHI pursuant to 45 C.F.R. § 164.522(b), provided that **ABC** notifies **Business Associate** in writing of the restriction or confidential communication obligations that **Business Associate** must follow. **ABC** will promptly notify **Business Associate** in writing of the termination of any such restriction agreement or confidential communication requirement, and with respect to termination of any such restriction agreement, instruct **Business Associate** whether any PHI will remain subject to the terms of the restriction agreement.

#### **D. Termination and Continuing Privacy and Security Obligations**

1. **Termination of Agreement.** As required by the HIPAA Regulations and this Agreement, **ABC** may, in addition to other available remedies, terminate the Agreement and this Agreement if **Business Associate** has materially breached any provision of this Agreement and has failed to cure or take actions to cure such material breach within five (5) calendar days of such breach. **ABC** shall exercise this right to terminate the Agreement by providing **Business Associate** written notice of termination, which shall include the reason for the termination. Any such termination shall be effective immediately or at such other date specified in **ABC's** notice of termination. Within thirty (30) calendar days of such termination of the Agreement, **Business Associate** shall provide to **ABC** one final report of any and all Breaches made of all individuals' PHI during the term of the Agreement.
  - a. **Obligations upon Termination.** Upon termination, cancellation, expiration or other conclusion of the Agreement, **Business Associate** shall immediately return or destroy all PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI, in whatever form or medium (including in any electronic medium under **Business Associate's** custody or control), and at whatever location the PHI resides including offices local and remote, data centers, remote storage facilities, off-site backup facilities and vendors, and all other locations, that **Business Associate** created or received for or from **ABC. Business Associate** as possible, but not later than thirty (30) calendar days



after the effective date of the termination, cancellation, expiration or other conclusion of the Agreement. **Business Associate** shall identify any PHI, including copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI created or received for or from **ABC** that cannot feasibly be destroyed or returned to **ABC**, and shall limit its further use or disclosure of such PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI. Within thirty (30) days of termination, cancellation, expiration or other conclusion of the Agreement, an officer of **Business Associate** shall certify in writing to **ABC** that such return or destruction has been completed, shall deliver to **ABC** the identification of any PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI, for which return or destruction is infeasible and, for that PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI, shall certify that it shall only use or disclose such PHI for those purposes that make return or destruction infeasible. All requirements of this section shall apply to any further **Business Associate** or vendor to whom **Business Associate** disclosed PHI.

2. Continuing Privacy and Security Obligation. **Business Associate** obligation to protect the privacy and security of the PHI, including all copies of and any data or compilations derived from and allowing identification of any individual who is a subject of the PHI, it created for or received from **ABC** shall be continuous and survive termination, cancellation, expiration or other conclusion of the Agreement.

**E. Indemnification and Hold Harmless.** **Business Associate** shall indemnify and hold harmless **ABC**, and **ABC** affiliates, subsidiaries, officers, directors, employees and agents from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees and court or proceeding costs, arising out of or in connection with any non-permitted or violating use or disclosure of PHI or other breach of this Agreement by **Business Associate** or any **Business Associate** subcontractor, agent, representative, person or entity. This Section E shall survive the termination of the Agreement.

**F. Conflicts.** The terms and conditions of this Agreement shall prevail in the event any terms and conditions herein conflict with any provision of the Agreement.

**G. ABC and Business Associate Privacy and Security Contact Information.**

**Privacy:**

**ABC**

Attn:

E-mail:

**VENDOR**

Attn:

Mailing Address:

City, State Zip:

Phone:

Email:

**Security:**

a. **ABC**

Attn:

Phone:

E-mail:

b. **VENDOR**

Attn:

Mailing

City, State Zip:

Phone:

Email:

Except as set forth in this Agreement, all other provisions of this Agreement shall remain unchanged and in effect.

**ABC**

**VENDOR**

Signature:

Signature: \_\_\_\_\_

Name:

Name

Title:

Title:

Date: \_\_\_\_\_

Date: