American Board of Internal Medicine®

HIPAA BUSINESS ASSOCIATE ADDENDUM
(Privacy & Security)

I. Definitions

A. **Business Associate.** "Business Associate" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 C.F.R. § 160.103, and in this case shall include the American Board of Internal Medicine, American Board of Allergy and Immunology, CECity.com, Inc. and their respective affiliates.

B. **Covered Entity.** "Covered Entity" shall have the meaning given to such term under the Privacy and Security Rules, including, but not limited to, 45 C.F.R. § 160.103, and in this case shall include any user of the website to which this Addendum relates.

C. **Designated Record Set**. "Designated Record Set" shall have the meaning given to such term under the Privacy Rule, codified at 45 C.F.R. § 164.501.

D. **Electronic Protected Health Information or "EPHI".** "Electronic protected health information" or "EPHI" shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 160.103.

E. **HIPAA**. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder, as each may be amended from time to time.

F. **HIPAA Breach**. "HIPAA Breach" shall have the meaning given to such term under the Privacy Rule, codified at 45 C.F.R. § 164.402.

G. **HITECH.** "HITECH" shall mean Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009; and the regulations promulgated thereunder, as may be amended from time to time.

H. **Individual**. "Individual" shall have the meaning given to such term under the Privacy Rule, codified at 45 C.F.R. § 160.103, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

I. **Law.** "Law" shall mean all federal and state statutes, together with their implementing regulations, that are applicable to services provided by Business Associate and activities conducted by Covered Entity under the Agreement.

J. **Privacy Rule**. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. Parts 160 and 164, subparts A and E.

K. **Privacy and Security Rules**. "Privacy and Security Rules" shall mean the federal regulations set forth at 45 C.F.R. Parts 160 and 164.

L. **Protected Health Information or "PHI"**. "Protected Health Information" or "PHI" shall have the meaning given to such term under the Privacy and Security Rules, codified at 45 C.F.R. § 160.103.

M. **Required by Law**. "Required by Law" shall have the meaning given to such term under the Privacy Rule, codified at 45 C.F.R. § 164.103.

N. **Secretary**. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or their designee.

O. **Security Rule**. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

P. **Unsecured PHI.** "Unsecured PHI" shall have the meaning given to such term under the Privacy Rule, codified at 45. C.F.R. § 164.402, but limited to the PHI created, received, maintained or transmitted by Business Associate on behalf of Covered Entity.

Q. Other terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in HIPAA or HITECH, as applicable.

II. Obligations and Activities of Business Associate

A. **Limitations on Disclosure**. Business Associate agrees to not use or disclose PHI other than as permitted or required by this Addendum or as Required by Law. Business Associate shall not use or disclose PHI in a manner that would violate the Privacy Rule if done by Covered Entity, unless expressly permitted to do so pursuant to the Privacy Rule and this Addendum.

B. **Safeguards**. Business Associate agrees to use appropriate safeguards to prevent use of disclosure of PHI other than as provided for by this Addendum or as required by law.

1. Business Associate agrees to comply with all privacy and security requirements applicable to business associates under HIPAA, HITECH and other applicable laws and regulations, including but not limited to the security rules under HIPAA ; requirements regarding the use of the minimum amount of PHI to achieve a particular purpose; the requirement to take appropriate action where Business Associate knows of a pattern of activity or practice by Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Addendum; restrictions on the sale or marketing of PHI; and acceptance of certain restrictions requested by individuals with respect to the disclosure of PHI for payment or health care operations purposes that were paid for entirely out-of-pocket.

2. In establishing the safeguards described in Section II.B, Business Associate shall, to the extent Business Associate in its sole discretion determines feasible, implement the following measures: (i) obtain, maintain, use and disclose PHI in a form that meets the requirements of a limited data set (where practical, without zip codes or

dates of birth); and (ii) apply guidance issued by the Secretary with regard to both the most effective and appropriate technical safeguards and the relevant standards and methodologies for preventing PHI from being treated as unsecured PHI.

C. **Mitigation**. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Addendum.

D. **Reporting of Disclosures**. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Addendum of becoming aware of such disclosure.

E. **Agents and Subcontractors**. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

F. **Access**. To the extent Business Associate has PHI in a Designated Record Set, Business Associate agrees to provide access to Covered Entity, at the request of Covered Entity, to PHI in a Designated Record Set, in order to meet the requirements under 45 C.F.R. § 164.524.

G. **Amendment**. To the extent Business Associate has PHI in a Designated Record Set and to the extent applicable**,** Business Associate agrees to make PHI in a Designated Record Set available to Covered Entity for purposes of amendment, per 45 C.F.R. § 164.526.

H. **Accounting**. To the extent applicable, Business Associate agrees to document disclosures of PHI 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 PHI in accordance with 45 C.F.R. § 164.528.

I. **Availability of Books and Records**. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

J. **Breach Notification**.

1. Business Associate agrees to take appropriate measures to prevent unauthorized disclosures of PHI. Business Associate agrees to identify potential breaches of PHI; upon discovery of a potential HIPAA Breach, Business Associate shall determine promptly whether the incident is an actual HIPAA Breach. Business Associate shall report each HIPAA Breach of Unsecured PHI to Covered Entity, all in accordance with the timing, content and other requirements of HITECH. Business Associate shall take appropriate measures to prevent such a breach from occurring in the future. Business Associate shall maintain appropriate records of its investigation of

potential HIPAA Breaches and responses to actual HIPAA Breaches in accordance with the documentation requirements of HIPAA and HITECH.

2. At Covered Entity's reasonable request, Business Associate shall provide Covered Entity with (i) information Covered Entity requires to meet its obligations under HIPAA and HITECH; and (ii) appropriate documentation of actions Business Associate has taken to comply with its obligations under this Section and under HIPAA and HITECH.

III. Obligations and Activities of Covered Entity

A. Authority to Disclose PHI. Covered Entity shall not disclose any PHI to Business Associate unless it has obtained any consents and authorizations that may be required by Law.

B. Compliance with Law. Covered Entity shall not disclose any PHI to Business Associate other than as permitted or required by the Agreement or by applicable Law.

C. Notice of Changes. Covered Entity shall notify Business Associate of any changes made to its Notice of Privacy Practices that may affect Business Associate's use of PHI and any restriction on the use or disclosure of PHI.

IV. Permitted Uses and Disclosures by Business Associate

A. Uses and Disclosures of PHI. Except as provided in Paragraphs B, C, D and E, below, Business Associate may only use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity to provide the features, information and services offered through the ABIM PIM Website and for the purposes of analysis, research and publication.

B. Use for Management and Administration. Except as otherwise limited in this Addendum, Business Associate may, consistent with 45 C.F.R. § 164.504(e)(4), use PHI if necessary (i) for the proper management and administration of the Business Associate, or (ii) to carry out the legal responsibilities of the Business Associate.

C. Disclosure for Management and Administration. Except as otherwise limited in this Addendum, Business Associate may, consistent with 45 C.F.R. § 164.504(e)(4), disclose PHI for the proper management and administration of the Business Associate, provided that (i) the disclosures are Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed ("Person") that it will remain confidential and be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the Person, and the Person notifies the Business Associate in writing of any instances of which it becomes aware in which the confidentiality of the information has been breached.

D. Data Aggregation. Except as otherwise limited in this Addendum, Business Associate may use PHI to provide Data Aggregation services as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B).

E. **De-Identification.** Business Associate may de-identify PHI received from Covered Entity, consistent with the Privacy Rule's standards for de-identification. 45 C.F.R. § 164.514.

F. **Reporting Violations**. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. § 164.502(j)(1).

V. Security Rule Obligations

A. **Business Associate Obligations**. Business Associate shall implement the requirements set forth in this Section IV with regard to EPHI.

B. **Safeguards.** Business Associate shall have in place Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the Confidentiality, Integrity, and Availability of the EPHI that it creates, receives, maintains or transmits on behalf of Covered Entity pursuant to the Addendum.

C. **Subcontractors**. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect such EPHI.

D. **Security Incident Reporting.** Business Associate shall report any Security Incident to Covered Entity promptly upon becoming aware of such incident.

VI. Term and Termination

A. **Term.** The Term of this Addendum shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI (as provided in Paragraph V(C) below), protections are extended to such information, in accordance with the termination provisions in this Section.

B. **Termination for Cause.** Upon discovery of a material breach of the terms of this Addendum by a party, the other party:

1. Shall provide an opportunity for the party to cure, and, if the party does not cure the breach within 30 days, the other party may immediately terminate this Addendum;

2. May immediately terminate this Addendum if the party has determined that (a) the other party has breached a material term of this Addendum, and (b) cure is not possible; or

3. If the party determines that neither termination nor cure are feasible, the party shall report the violation to the Secretary.

C. **Effect of Termination.**

1. Except as provided below in Paragraph 2 of this Section, upon termination of this Addendum, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate and Business Associate is obligated to ensure that such PHI is returned or destroyed consistent with this Addendum. Business Associate and its subcontractors or agents shall retain no copies of the PHI.

2. Where Business Associate asserts that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon Business Associate's good faith representations that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Addendum to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VII. Miscellaneous

A. **Regulatory References.** A reference in this Addendum to a section in HIPAA or HITECH, as applicable, means the section as in effect at the relevant time.

B. **No Third Party Beneficiaries.** Nothing expressed or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity and Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

C. **Disclaimer.** Business Associate makes no warranty or representation that compliance by Covered Entity with this Addendum is satisfactory for Covered Entity to comply with any obligations it may have under HIPAA, HITECH, or any other applicable law or regulation pertaining to the confidentiality, use or safeguarding of health information. Covered Entity is solely responsible for all decisions it makes regarding the use, disclosure or safeguarding of PHI.