

This Business Associate Agreement (the “Agreement”) is made effective on _____, 20____, (“Effective Date”) by and between IT Solutions Consulting, Inc. (the “Business Associate”) and its client _____ (the “Covered Entity”).

Background

The HIPAA Privacy Rule applies only to “Covered Entities” – health plans, health care clearinghouses, and certain health care providers. However, most health care providers use the services of a variety of other persons or businesses.

The Privacy Rule allows covered providers and health plans to disclose protected health information to “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity’s duties under the Privacy Rule.

The Covered Entity has contracted, or intends to contract, with the Business Associate for managed IT services. As a component of such services, protected health information may be disclosed to the Business Associate in the ordinary course of business.

Accordingly, this Agreement is intended to comply with HIPAA’s requirements in order for our client which is a Covered Entity to lawfully disclose protected health information to IT Solutions Consulting, Inc., the Business Associate, for the purposes described above.

Agreement

I. Definitions

Catch-all definition: The terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules, even when not expressed in capitalized terms.

Specific definitions:

- (a) “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean IT Solutions Consulting, Inc.
- (b) “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this Agreement, shall mean our client named above.
- (c) “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164. “Privacy Rule” means that portion of HIPAA set forth in 45 CFR Part 160 and Part 164, Subparts A and E.

- (d) “Data Aggregation” means, with respect to PHI created or received by Business Associate in its capacity as the “business associate” under HIPAA of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a Business Associate of one or more other “Covered Entity” under HIPAA, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of “data aggregation” in this Agreement shall be consistent with the meaning given to that term in the Privacy Rule.
- (e) “Designated Record Set” has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501.B.
- (f) “De-Identify” means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).
- (g) “Electronic PHI” means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.
- (h) “Health Care Operations” has the meaning given to that term in 45 CFR §164.501.
- (i) “HHS” means the U.S. Department of Health and Human Services.
- (j) “HITECH Act” means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.
- (k) “Individual” has the same meaning given to that term in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- (l) “Protected Health Information” or “PHI” has the meaning given to the term “protected health information” in 45 CFR §§164.501 and 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- (m) “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.
- (n) “Security Rule” means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.
- (o) “Unsecured Protected Health Information” or “Unsecured PHI” means any “protected health information” as defined in 45 CFR §§164.501 and 160.103 that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in the guidance issued pursuant to the HITECH Act and codified at 42 USC §17932(h).

II. Obligations and Activities of Business Associate

The Business Associate agrees to:

- (a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law.
- (b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement.
- (c) Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which Business Associate becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware, no later than five (5) business days of becoming aware of such event.

Such reporting shall be in accord with the protocols of the Client Agreement between Covered Entity and Business Associate, unless otherwise called for by law. Such protocols, including terms on timing, shall control in the event of any conflict with this Subsection II.(c).

The Business Associate shall not have any obligation to notify individuals, other persons, or the media regarding such events.

- (d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.
- (e) Make available protected health information in a designated record set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524.

The Business Associate will not have any obligation to respond to an individual request for information access and shall notify Covered Entity within ten (10) business days of any such request in order for the Covered Entity to fulfill the request and direct Business Associate accordingly. Business Associate will follow any and all reasonable directives from Covered Entity regarding provision of access to information to requesting individuals.

- (f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526.

The Business Associate will not have any obligation to respond to an individual request for information amendment and shall notify Covered Entity within ten (10) business days of any such request in order for the Covered Entity to fulfill the request and direct Business Associate accordingly. Business Associate will follow any and all reasonable directives from Covered Entity regarding amendment of information or to record sets.

- (g) Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy covered entity's obligations under 45 CFR 164.528.

The Business Associate will not have any obligation to respond to an individual request for an accounting and shall notify Covered Entity within ten (10) business days of any such request in order for the Covered Entity to fulfill the request and direct Business Associate accordingly. Business Associate will follow any and all reasonable directives from Covered Entity regarding provision of accounting information to requesting individuals.

- (h) To the extent the business associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and
- (i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

III. Permitted Uses and Disclosures by Business Associate

- (a) Business Associate may only use or disclose protected health information as necessary to perform the services set forth in Client Agreement. The Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c), if in furtherance of the services set forth in the Client Agreement.
- (b) Business Associate may use or disclose protected health information as required by law.
- (c) Business Associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.
- (d) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity, except for the specific uses and disclosures set forth below.
- (e) Business Associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

- (f) Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (g) Business Associate may provide data aggregation services relating to the health care operations of the Covered Entity.

IV. Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

- (a) Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.
- (b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.
- (c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

V. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity, except using protected health information for, provided the Client Agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the Business Associate.

VI. Term and Termination

Termination of this Agreement shall be in accord with the following provisions:

- (a) Term. The Term of this Agreement shall be effective as of Effective Date, and shall terminate on the date the underlying Client Agreement terminates, or on the date Covered Entity

terminates this Agreement for cause as authorized in paragraph (b) of this Section, or on another date agreed in writing by the parties hereto, whichever is sooner.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement and Business Associate has not cured the breach or ended the violation within thirty (30) days from written notice by Covered Entity.

(c) Obligations of Business Associate Upon Termination. Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Business Associate will be returned to Covered Entity or destroyed by Business Associate. Business Associate will not retain any copies of such information. This provision will apply to PHI in the possession of Business Associate's agents and subcontractors. If return or destruction of the PHI is not feasible, in Business Associate's reasonable judgment, Business Associate will furnish Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of the PHI is infeasible, Business Associate will extend the protections of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The Parties understand that this Section 14.D. will survive any termination of this BAA.

Covered Entity acknowledges that Business Associate's managed IT services provides access to Covered Entity's data environment, but does not typically involve Business Associate's physical hosting, taking, maintaining, exercising dominion or control over, or otherwise possessing Covered Entity's data or files. Covered Entity acknowledges that, upon termination, Business Associate's withdrawing from access to and management of Covered Entity's data, including technical access to any PHI, will constitute compliance with this Article VI, will constitute "returning" of PHI to Covered Entity as contemplated above, and will discharge any and all obligations of Business Associate under HIPAA Rules.

(d) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

Miscellaneous

- (a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.
- (b) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.
- (c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

- (d) Third-parties. Except as expressly stated herein or as provided by law, this Agreement will not create any rights in favor of any third party.
- (e) HITECH Act Compliance. The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements for business associates and the agreements between business associates and covered entities under HIPAA and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this Agreement as reasonably necessary to comply with the HITECH Act and its regulations as they become effective but, in the event that the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this Agreement upon 30-days' prior written notice to the other Party.

CLIENT

IT SOLUTIONS CONSULTING, INC.

Name/Title:

Date:

[ADD A STOCK SIGNATURE OR IMAGE]

Name/Title:

Date: