



HIPAA Business Associate Agreement Instructions

HIPAA AND COLA ACCREDITATION

The Health Insurance Portability and Accountability Act (HIPAA) requires laboratories to enter into written agreements with their business associates, defined as any entity that may have access to protected health information (PHI) as a result of services provided to the laboratory.

Since the COLA accreditation program includes an onsite visit and review of records and documentation, COLA falls into the definition of a Business Associate. It is therefore necessary that COLA accredited laboratories enter into a Business Associate Agreement (BAA) with COLA.

If your facility has its own BAA, please send it to COLA for signature. If your facility does not have its own BAA, COLA has a model BAA that includes the requirements known as "HITECH" issued by the Office of Civil Rights (OCR) in January, 2013.

IMPORTANT: if you are currently using a prior version of COLA's model agreement we urge you to use the new updated version that includes HITECH instead.

INSTRUCTIONS:

Please send your HIPAA Business Associate Agreement, including your COLA identification number, or for multiple locations, all COLA numbers, to any of the following:

FAX to 410-381-8611

COLA
HIPAA Compliance Department
9881 Broken Land Parkway, Suite 200
Columbia, MD 21046

You may also obtain a copy either through our website, www.cola.org or through COLAcentral® once you have set up your account.



BUSINESS ASSOCIATE AGREEMENT

In order to comply with the Health Insurance Portability and Accountability Act of 1996, Subtitle D of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), and all regulations and guidance promulgated thereunder (collectively "HIPAA"), this Business Associate Agreement (this "Agreement") is made and entered into by and between

(the "Covered Entity")

and COLA Inc. (the "Business Associate"). This Agreement supersedes any previous business associate agreements between the parties.

1. DEFINITIONS.

- a. "Breach" shall have the meaning given to the term "breach" at 45 C.F.R. § 164.402.
- b. "ePHI" shall have the meaning given to the term "electronic protected health information" under the Security Rule at 45 C.F.R. § 160.103, as applied to the information created, received, maintained, or transmitted by the Business Associate from or on behalf of Covered Entity.
- c. "Individual" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 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).
- d. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
- e. "Protected Health Information" or "PHI" shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity.
- f. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.
- g. "Subcontractor" shall have the meaning given to the term "subcontractor" at 45 C.F.R. § 160.103.
- h. Any other terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in HIPAA. Any inconsistency in the definition of a capitalized term shall be resolved in favor of a meaning that permits compliance with HIPAA.

2. PERMITTED USES AND DISCLOSURES OF PHI. Except as otherwise limited in this Agreement, Business Associate may do any or all of the following:

- a. Use or Disclosure Under Agreement. Use or disclose PHI to perform laboratory testing, inspection, accreditation services and/or other services for Covered Entity, provided that such use or



disclosure would not violate any applicable state law or the Privacy Rule if done by Covered Entity. Notwithstanding the foregoing, Business Associate may use and disclose PHI for purposes identified in Section 2(b) and (c) of this Agreement. Business Associate agrees not to use or disclose PHI other than as permitted or required by the Agreement or as Required by Law.

b. Use for Administration. Use PHI, but only to the minimum extent necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

c. Disclosure for Administration or as Legally Required. Disclose PHI, but only to the minimum extent necessary for the proper management and administration of Business Associate, or to carry out the legal responsibilities of 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 that it shall remain confidential and shall be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, agent, or other entity including a Subcontractor (which purpose must be consistent with the limitations imposed upon Business Associate pursuant to this Agreement), and that the person, agent, or other entity, including a Subcontractor, agrees to promptly notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Use for Reporting of Violations. Use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(l).

e. Use for Data Aggregation Services. Use PHI to provide Data Aggregation services relating to the health care operations of Covered Entity, as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), but only if requested by Covered Entity in writing.

3. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE.

a. Limited by this Agreement and Law. Business Associate may not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

b. Compliance with HIPAA. To the extent that Business Associate is, pursuant to this Agreement, responsible for carrying out an obligation of Covered Entity under HIPAA, Business Associate shall comply with the requirements of HIPAA that apply to Covered Entity in the performance of such obligation.

c. Appropriate Safeguards. Business Associate shall use appropriate safeguards and, where applicable, comply with the Security Rule with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.

d. Reporting of Improper Use or Disclosure. Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for by this Agreement, including Breaches of Unsecured PHI as required at 45 C.F.R. § 164.410, and any Security Incident without unreasonably delay after becoming aware of such use or disclosure or Security Incident and, with regard to a Breach, in no event later than forty-five (45) days following a Discovery of such Breach. In the case of a Breach, Business Associate shall provide Covered Entity with the information required pursuant to 45 C.F.R. § 164.410(c).

e. Subcontractors. If Business Associate discloses PHI to a Subcontractor or allows a Subcontractor to create, receive, maintain, or transmit PHI or ePHI on its behalf, Business Associate must, in accordance with 45 C.F.R. §§ 164.308(b)(2), and 164.502(e)(1)(ii), ensure that such Subcontractor agrees to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information by entering into a written arrangement with Subcontractor that complies with 45 C.F.R. §§ 164.314(a) and 164.504(e). If Business Associate becomes aware of a pattern of activity or practice of a Subcontractor that would constitute a material Breach or violation of the written agreement between Business Associate and Subcontractor, Business Associate shall (1) take reasonable steps to cure such Breach or end the violation, as applicable, or terminate such written agreement with such Subcontractor, and (2) promptly report such material Breach or violation by the Subcontractor to Covered Entity in writing.

f. Access to PHI. To the extent that Business Associate maintains PHI in a Designated Record Set, Business Associate shall provide access to such PHI to Covered Entity in the time and manner that meets the requirements of 45 C.F.R. § 164.524.

g. Amendment of PHI. To the extent that Business Associate maintains PHI in a Designated Record Set, Business Associate shall make amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to, at the request of Covered Entity, and in the time and manner that meets the requirements of 45 C.F.R. § 164.526.

h. Accounting of Disclosures. Business Associate shall provide to Covered Entity an accounting of the disclosures of an Individual's PHI, and in a time and manner that meets the requirements of 45 CFR § 164.528 and, as of the applicable effective date, Section 13405(a) of HITECH.

i. Governmental Access to Records. Business Associate shall make its internal practices, books and records 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 for purposes of the Secretary determining Covered Entity's compliance with HIPAA. No attorney-client, accountant-client, or other legal privilege shall be deemed to have been waived by Covered Entity or Business Associate by virtue of Business Associate's compliance with this provision.

j. Mitigation. Business Associate agrees to mitigate, to the extent practicable and required by law, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate (or by any other person to whom Business Associate has disclosed PHI) in violation of the requirements of this Agreement.

k. Minimum Necessary. Business Associate agrees that, to the extent practicable, it shall only request, use and disclose PHI in the form of a limited data set (as defined in 45 C.F.R. § 164.514(e)(2)), and that in all other cases it shall only request, use or disclose the minimum necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure. The parties recognize that it is the responsibility of the Covered Entity to determine whether the requested data is minimally necessary, and Covered Entity agrees not to disclose any PHI that is not minimally necessary to Business Associate.



l. Communicate with Other Business Associates. In connection with the performance of its services, activities, and/or functions to or on behalf of Covered Entity, Business Associate may disclose information, including PHI, to other business associates of Covered Entity that have been identified in writing by Covered Entity. Likewise, Business Associate may use and disclose information, including PHI, received from other business associates of Covered Entity, as if this information was received from, or originated with, Covered Entity.

m. Documentation. All documentation that is required by this Agreement and HIPAA shall be retained by Business Associate for six (6) years from the date of creation or when it was last in effect, whichever is later.

4. OBLIGATIONS OF COVERED ENTITY.

a. Notice of Privacy Practices. Covered Entity acknowledges that it is solely responsible for developing, updating and providing a notice of privacy practices, on behalf of itself, in accordance with 45 C.F.R. § 164.520. Covered Entity shall notify Business Associate of any limitations in its notice of privacy practices, to the extent that such limitations may affect Business Associate's use or disclosure of PHI.

b. Notification of Revocations. Covered Entity shall notify Business Associate of any changes in, or revocation of, authorization by an Individual to use or disclose PHI, to the extent that such changes or revocation may affect Business Associate's use or disclosure of PHI.

c. Notification of Restrictions. Covered Entity covenants and agrees that it shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to, or is required to abide by, in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

d. Permissible Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

5. TERM AND TERMINATION.

a. Term. The term of this Agreement shall commence as of the date hereof, and shall continue in full force and effect from year-to-year, but shall terminate as of the earliest of (i) the termination of the business relationship between the parties, (ii) the termination of this Agreement for cause as described in Section 5(b), (iii) the termination of this Agreement by mutual agreement of the parties, or (iv) the termination of this Agreement under applicable federal, state or local law.

b. Termination for Cause. Upon either party's determination of a Breach of a material term by the other party, the non-Breaching party shall provide the Breaching party with written notice of that Breach in sufficient detail to enable the Breaching party to understand the specific nature of that Breach and afford the Breaching party an opportunity to cure the Breach; provided, however, that if the Breaching party fails to cure the Breach within thirty (30) days of receipt of such notice, the non-Breaching party may terminate this Agreement.

c. Effect of Termination

(i) Upon termination of this Agreement for any reason, Business Associate shall return or destroy, all PHI received from, or created, received, maintained, or transmitted by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form, as well as the documentation required by 45 C.F.R. § 164.530(j)(1) (all of which shall be collectively referred to as PHI for purposes of this Section 5(c)(i)). Business Associate shall retain no copies of such PHI.

(ii) If return or destruction of all PHI is not feasible, Business Associate shall:

(1) Retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(2) Return to Covered Entity or destroy the remaining PHI that Business Associate still maintains in any form;

(3) Extend the protections of this Agreement to any retained PHI, continue to use appropriate safeguards, and comply with the Security Rule with respect to ePHI in order to prevent use or disclosure of the retained PHI other than as provided for in this Section 5(c)(ii), for as long as Business Associate retains the PHI;

(4) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set forth in Section 2(b) of this Agreement that applies prior to termination; and

(5) Return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

(iii) These provisions shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate.

(iv) Business Associate shall certify to Covered Entity that it has destroyed or returned all such PHI requested to be destroyed or returned, as the case may be.

(v) Any PHI that Business Associate destroys shall be destroyed in accordance with HIPAA.

6. MISCELLANEOUS.

a. Amendment; No Waiver. This Agreement shall be automatically amended to comply with any changes made to HIPAA after the date of execution of this Agreement, unless the parties agree by mutual consent not to have the Agreement automatically amended. The parties shall take all necessary action to reflect automatic amendments from time to time. Except as provided above, no waiver, change, modification, or amendment of any provision of this Agreement shall be made unless it is in writing and is signed by the parties hereto. The failure of either party at any time to insist upon strict performance of any condition, promise, agreement or understanding set forth herein shall not be



construed as a waiver or relinquishment of the right to insist upon strict performance of the same condition, promise, agreement or understanding at a future time.

b. Headings. The titles and headings set forth at the beginning of each Section hereof are inserted for convenience of reference only and shall in no way be construed as a part of this Agreement or as a limitation on the scope of the particular provision to which it refers.

c. Survival. All of the respective rights and obligations of Business Associate under Section 3(m) and Section 5(c) of this Agreement shall survive the termination of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with HIPAA. In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of HIPAA, as may be expressly amended from time-to-time by the Secretary, or as a result of interpretations by the Secretary, a court, or another regulatory agency with authority over the parties, the interpretation of the Secretary, such court, or regulatory agency shall prevail.

e. Invalid or Unenforceable Provision. The provisions of this Agreement shall be severable. The invalidity or unenforceability of any particular provision of this Agreement shall be construed, in all respects, as if such invalid or unenforceable provision had been omitted, and shall not affect the validity and enforceability of the other provisions hereof.

f. Nonassignability: Benefits and Burdens. Neither party may assign its rights, or delegate its duties or obligations, under this Agreement without the prior written consent of the other party, which consent shall not be unreasonably withheld. This Agreement shall be binding upon, and shall inure to the benefit of, the parties hereto and their respective successors.

g. Governing Law. Except to the extent preempted by applicable federal law, this Agreement shall be construed, administered and governed under the laws of State of Maryland.

h. Entire Agreement. This Agreement constitutes the entire agreement between Covered Entity and Business Associate with respect to the matters described herein. Any prior agreements, statements, promises, negotiations, inducements, or representations, either oral or written, made by either party or agent of either party, that are not contained in this Agreement shall be of no force or effect.

i. Notices. All notices hereunder shall be in writing, and either delivered by hand, or sent by mail, or delivered in such other manner as the parties may agree upon, to the addresses listed on the signature page.

j. Counterparts. This Agreement may be executed in separate counterparts, none of which need contain the signatures of both parties, and each of which, when so executed, shall be deemed to be an original, and such counterparts shall together constitute and be one and the same instrument.



k. No Third Party Beneficiaries. This Addendum is between the parties hereto. 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, any rights, remedies, obligations or liabilities whatsoever.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of _____

COVERED ENTITY:

By entering my name below, I attest that I have the authority to enter this agreement and agree to be bound by the terms.

By: _____

Name: _____

Title: _____

Address: _____

Date: _____

COLA ID #(s): _____

(attach list if necessary)

BUSINESS ASSOCIATE:

COLA, Inc.

By: _____

Name: _____

Title: _____

Address: COLA, Inc.

9881 Broken Land Parkway

Suite 200

Columbia, MD 21046

Date: _____