California Dental Association
1201 K Street, Sacramento, CA 95814
800.232.7645 cda.org

HIPAA Business Associate Agreement

The compliance date for the 2013 HIPAA amendments is September 23, 2013. Recognizing that some covered entities and business associates need additional time to re-open and revise existing contracts, the Department of Health and Human Services is allowing additional time, until September 23, 2014, to bring into compliance the written business associate agreements that were in effect on January 25, 2013 (the publication date of the amendments). The transition provision only applies to the amendment of existing agreements and not to other newer requirements such as business associate compliance with the Privacy Rule. This sample agreement includes the required revisions.

The following resource is provided by CDA for informational purposes only and should not be considered legal advice. Appropriate legal advice regarding a particular question or specific situation should be obtained by you from qualified legal counsel.

HIPAA requires a covered entity to have a business associate agreement with any entity, individual, or organization that creates, receives, maintains, or transmits patient health information to perform nonclinical functions, such as claims processing or information systems management, on behalf of a covered entity. A dental practice that is a covered entity must have a business associate agreement with each entity that uses its patients' information for nonclinical functions. Examples of dental practice business associates include:

- Claims clearinghouse
- Practice management software vendor
- Electronic file sharing service
- Online data back-up and storage service
- Practice management consultant
- Malpractice insurer
- Attorney
- Accountant

Consider if you need a business associate agreement with another dentist with whom you share space but not patients. An agreement is necessary if you utilize another dentist's employees to file claims, collect from your patients, or contact your patients.

Obtain an agreement from a business associate before providing the entity with access to patient information. Some business associate agreements may be for an extended period, for example with a claims clearinghouse or a practice management software vendor that has regular access to patient information. Other business associate agreements can be for a shorter term, for example with a malpractice carrier upon filing a claim or seeking risk management assistance, or with an accountant who is assisting the dental practice on how to respond to an IRS request for information or conducting a practice valuation.

Subcontractors of business associates are now considered business associates under HIPAA.

Although health information exchange organizations, regional health information organizations, and e-prescribing gateways are not commonly used by dental practices, you should know that business associate agreements with these entities must be in place if they are used.

Not Business Associates: Dental laboratories, other dentists to whom you refer or receive referrals from, and the practice workforce, that includes employees, students and interns, are not business associates. Independent contractors may be considered as part of the practice's workforce. Researchers are not business associates; however, patient authorization to use limited data set is required. The U.S. Postal Service, couriers, internet service providers, and other organizations that transmit patient health information but do not maintain or routinely access patient health information also are not business associates.

Additionally, California law requires you to obtain specific patient authorization to share patient information with those business associates who are not third-party payers; entities who require access to the information in liability, arbitration, peer review, quality assurance, quality assessment, or medical necessity cases; or otherwise not included in Civil Code section 56.10.

What to include in a Business Associate Agreement: A covered entity must obtain satisfactory assurances from a business associate that it will safeguard patient information according to standards of the Privacy and Security Rules. The business associate agreement (which can be part of a contract for services) should contain the following elements, according to the Department of Health and Human Services. (hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html):

Business associates may use and disclose the patient information provided by the covered entity **only** as provided for in the agreement and as allowed by law. With the business associate agreement, a covered entity may further clarify and limit the permissible uses and disclosures by the business associate and may set additional requirements for the business associate. For example, a covered entity may want to detail how it and the business associate will coordinate the reporting of a breach at the business associate.

1. establish the permitted and required uses and disclosures of protected health information by the business associate;
2. provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law;
3. require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the Security Rule;
4. require the business associate to report to the covered entity any use or disclosure of the information not provided for by its agreement, including incidents that constitute breaches of unsecured protected health information;
5. require the business associate to disclose protected health information as specified in its agreement to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;
6. to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;
7. require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the Privacy Rule;
8. at termination of the business relationship, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of the covered entity;
9. require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
10. authorize termination of the agreement by the covered entity if the business associate violates a material term of the agreement.

Instructions for the Dental Practice

It is the covered entity's responsibility to obtain a business associate agreement. However, some organizations, such as TDIC and CDA, provide a covered entity with an agreement. In such instances, be sure to review the provided agreement and ensure it includes the required elements listed above. Ideally, the agreement should be reviewed by your attorney.

The following sample business associate agreement includes the required elements.

Fill in the blanks and provide a signed copy to your business associate. Obtain the signed business associate agreement before providing the business associate with access to patient information. Retain terminated business associate agreements for six years after date of termination.

June 2013

Sample HIPAA Business Associate Agreement

This **Business Associate Agreement** ("Agreement") is entered into this ___ day of _____, _____ between [_____], a California _____[state organization type] ("Covered Entity") and _____, a _____[state organization type] ("Business Associate").

Recitals

Covered Entity is a _____[state organization type] that provides dental services with a principal place of business at _____[address].

Business Associate is a _____[type of organization] that _____[describe functions and activities] with a principal place of business at _____[address].

Business Associate provides certain services ("Services") to Covered Entity pursuant to the Underlying Agreement.

Covered Entity is a "covered entity" as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (as amended, and including 45 CFR Pts 160 and 164 and any other regulations promulgated thereunder, all as of the date of this Agreement, "HIPAA").

In connection with Business Associate providing services to Covered Entity, Covered Entity may disclose to Business Associate certain Protected Health Information (as defined below) of patients, residents, or customers of Covered Entity that is protected under HIPAA and Subtitle D of Title XIII of Division A of the American Recovery and Reinvestment Act of 2009 (as amended, and including all regulations promulgated thereunder, all as of the effective date of this Agreement, "HITECH").

Business Associate, to the extent that it receives Protected Health Information from or on behalf of Covered Entity, is a "Business Associate" of Covered Entity as that term in defined under HIPAA and HITECH.

In order to ensure that Covered Entity, and, to the extent applicable, Business Associate, are in compliance with their respective obligations under HIPAA and HITECH, the parties have agreed to enter into this agreement.

Agreement

NOW, THEREFORE, in consideration of the mutual promises and covenants set forth in this Agreement, the parties agree as follows:

1. Definitions.

Unless otherwise defined in this Agreement, capitalized terms shall have the same meanings as set forth in HIPAA or HITECH, as applicable:

Breach.

(a) Breach. For purposes of Sections 3(g) and 3(l) of this Agreement only, "Breach" shall have the meaning set forth in 45 C.F.R. § 164.402 (including all of its subsections); with respect to all other uses of the word "breach" in this Agreement (e.g., Section 5), the word "breach" shall have its ordinary contract meaning.

Individual.

(b) Individual. “Individual” shall have the same meaning as the term “individual” in 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).

Protected Health Information.

(c) Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, limited to the information received from, or created or received by Business Associate from or on behalf of, Covered Entity.

Required By Law.

(d) Required By Law. “Required By Law” shall have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.

Secretary.

(e) Secretary. “Secretary” means the Secretary of the Department of Health and Human Services or his/her designee.

2. Scope of Use and Disclosure of Protected Health Information:

(a) Except as otherwise expressly limited in this Agreement or the Underlying Agreement, Business Associate may Use or Disclose Protected Health Information to perform all functions, activities or services for, or on behalf of, Covered Entity in connection with the Underlying Agreement, provided that such Use or Disclosure would not violate HIPAA (including the minimum necessary standard set forth in 45 C.F.R. § 164.502(b)) if done by Covered Entity.

(b) Except as otherwise expressly limited in this Agreement or the Underlying Agreement, Business Associate may Disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate if (1) the Disclosure is Required By Law, or (2) Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will remain confidential and will be Used or further Disclosed only as Required By Law or for the purpose for which it was Disclosed to such person, and the person agrees to notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) If requested by Covered Entity in writing, Business Associate may Use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).

(d) Business Associate may Use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3. Obligations of Business Associate with Respect to Protected Health Information:

(a) Business Associate shall Use and Disclose Protected Health Information only as permitted or required by this Agreement or as Required By Law.

(b) Business Associate shall use appropriate safeguards to prevent Use or Disclosure of the Protected Health Information other than as provided for by this Agreement.

(c) Business Associate shall implement administrative, physical and technical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains or transmits to or on behalf of Covered Entity as required by HIPAA.

(d) Business Associate agrees to provide access, at the request of Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

(e) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual.

(f) Business Associate shall mitigate, to the extent reasonably practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(g) Business Associate shall report to Covered Entity: (1) any Security Incident respecting electronic Protected Health Information within __ business days after Business Associate becomes aware of such Security Incident; and (2) any event not subject to reporting under the preceding Section 3(g)(1) of which Business Associate becomes aware that is not permitted or required by this Agreement. Notwithstanding the foregoing and for the avoidance of doubt, notifications pertaining to Breaches of Unsecured Protected Health Information shall be made as stated in Section 3(l) below, and not as stated in this Section 3(g).

(h) Business Associate shall enter into a written agreement with any agent or subcontractor to whom it provides Protected Health Information, which agreement shall include and require that such agent or subcontractor comply with the same restrictions and conditions that apply under this Agreement to Business Associate with respect to such Protected Health Information. If Business Associate becomes aware of a pattern or practice of activity of an agent or subcontractor that would constitute a material breach or violation of the written agreement between Business Associate and such agent or subcontractor, Business Associate shall take reasonable steps to cure such breach or terminate such written agreement with such agent or subcontractor.

(i) Business Associate shall make its internal practices, books, and records relating to the Use and Disclosure of Protected Health Information available to the Secretary in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA.

(j) Individuals' Access to PHI:
   (1) Business Associate shall coordinate with Covered Entity to appropriately respond to all requests for access to an individual's PHI that are approved by Covered Entity. Business Associate shall cooperate with Covered Entity in all respects necessary for Covered Entity to comply with 45 CFR 164.524 and California law. Business Associate agrees that to the extent Business Associate maintains PHI of Covered Entity in an electronic health record (EHR), the Covered Entity must comply with an individual's request for access to their PHI by giving them, or any entity that they clearly and specifically designate, the information in an electronic format if it is readily producible in such format. If it is not readily producible in such format, Business Associate will produce the PHI in a readable electronic format agreed to by the individual.
   (2) California law requires that copies of requested records be provided to patients within fifteen (15) days. Business Associate agrees to provide any copies requested by Covered Entity within five (5) business days. Business Associate shall forward any requests it receives from an individual for access to PHI to Covered Entity. Covered Entity is responsible for determining the scope of PHI and Designated Record Set for each request by an individual for access to PHI. Covered Entity will reimburse Business Associate for any costs incurred by Business Associate related to producing the requested records.

(k) Accounting of Disclosures:
  (1) Business Associate shall document Disclosures by Business Associate of Protected Health Information 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 Protected Health Information in accordance with 45 C.F.R. § 164.528. This provision does not cover disclosures of Protected Health Information that may result from Covered Entity's inappropriate choices of security settings or inappropriate usage of Business Associate's services.
  (2) Business Associate shall provide to Covered Entity or an Individual, within five business days of a request by Covered Entity, information collected in accordance with Section 3(j)(1) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of Disclosures of Protected Health Information in accordance with 45 C.F.R. § 164.528.

(l) Notifications Regarding Breaches of Unsecured Protected Health Information:
  (1) Following Business Associate's discovery (as described in 45 C.F.R. § 164.410(a)(2)) of a Breach of Unsecured Protected Health Information, Business Associate shall notify Covered Entity of such Breach in accordance with 45 C.F.R. §§ 164.410 and 164.412.
  (2) Business Associate shall establish reasonable systems to detect Breaches of Unsecured Protected Health Information and to provide appropriate training to its workforce regarding Business Associate's policies and procedures pertaining to Use and Disclosure of Protected Health Information and the detection and reporting of Breaches of Unsecured Protected Health Information.

(m) For purposes of paragraph (1) of § 13405(b) of HITECH, in the case of the Disclosure of Protected Health Information, the party (Covered Entity or Business Associate) Disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such Disclosure.

4. Obligations of Covered Entity:

(a) Covered Entity represents and warrants to Business Associate that it: (1) has included, and will include, in Covered Entity's Notice of Privacy Practices that Covered Entity may disclose Protected Health Information for health care operations purposes; and (2) has obtained, and will obtain, from Individuals, consents, authorizations and other permissions necessary or required by all laws applicable to Covered Entity for Business Associate and Covered Entity to fulfill their obligations under the Underlying Agreement and this Agreement.

(b) Covered Entity shall promptly notify Business Associate in writing of any restrictions on the Use and Disclosure of Protected Health Information about Individuals that Covered Entity has agreed to that could reasonably be expected to affect Business Associate's ability to perform its obligations under the Underlying Agreement or this Agreement.

(c) Covered Entity shall notify Business Associate in writing of any limitations in its notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that the limitations may affect Business Associate's Use or Disclosure of Protected Health Information.

(d) Covered Entity shall promptly notify Business Associate in writing of any changes in, or revocation of, permission by an Individual to Use or Disclose Protected Health Information, if such changes or revocation could reasonably be expected to affect Business Associate's ability to perform its obligations under the Underlying Agreement or this Agreement.

(e) Covered Entity shall utilize Business Associate's services in a way that ensures that Covered Entity is in compliance with HIPAA and HITECH.

(f) Covered Entity shall not request Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA or HITECH if done by Covered Entity, except to the extent that Business Associate is Using or Disclosing Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B),

and/or to the extent that Business Associate is Using or Disclosing Protected Health Information for the proper management and administration of Business Associate.

(g) Covered Entity shall use its best efforts to minimize the disclosure of Protected Health Information to Business Associate where the disclosure of that information is not needed for Business Associate to provide products or services to Covered Entity.

(h) Covered Entity agrees to indemnify and hold harmless Business Associate, its directors, officers, shareholders, parents, subsidiaries, affiliates, and agents, from and against all losses, expenses, damages and costs, including reasonable attorneys' fees, resulting from Covered Entity's failure to fulfill its obligations under the Underlying Agreement or this Agreement, including without limitation resulting from Covered Entity's failure to use Business Associate's services in such a manner as to prevent the unauthorized Disclosure of Protected Health Information.

5. Term and Termination:

(a) Term. This Agreement shall become effective as of the Effective Date and terminate upon the earlier of (1) termination of all the Underlying Agreement or (2) termination of this Agreement as provided herein.

(b) Termination. In the event of either party's material breach of this Agreement, the non-breaching party may terminate this Agreement upon 10 days prior written notice to the breaching party in the event the breaching party does not cure such breach to the reasonable satisfaction of the non-breaching party within such 10 day period. In the event that cure of a breach under this Section 5(b) is not reasonably possible, the non-breaching party may immediately terminate this Agreement; or if neither termination nor cure is feasible, the non-breaching party may report the violation to the Secretary.

6. Miscellaneous:

(a) Changes to Laws. If HIPAA and/or HITECH are amended (including, without limitation, by way of anticipated regulations yet to be promulgated as provided in HITECH), or if new laws and/or regulations affecting the terms required to be included in business associate agreements between covered entities and business associates are promulgated, and either party determines that modifications to the terms of this Agreement are required as a result, then promptly following a party's request, the parties shall engage in good faith negotiations in an effort to arrive at mutually acceptable changes to the terms set forth in this Agreement that address such amended or new law and/or regulation. If the parties are unable to agree on such modifications following a reasonable period of such good faith negotiations, which shall in no case extend beyond the effective date of such amended or new law and/or regulations, then any party that would become noncompliant in the absence of such modifications shall have the right to terminate this Agreement, and the provisions of Section 5(c) shall then apply.

(b) Notices. Any notice required or permitted under this Agreement shall be given in writing to Covered Entity at: contact information on file with Business Associate; to Business Associate at: _____. Notices will be deemed to have been received upon actual receipt, one business day after being sent by overnight courier service or facsimile, or three business days after mailing by first-class mail, whichever occurs first.

(c) Governing Law. This Agreement shall be governed by, and construed in accordance with, the laws of the State of California.

(d) Survival. The obligations of Business Associate under Section 3(j), Section 3(k) and Section 5 of this Agreement shall survive any termination of this Agreement.

(e) Amendments. This Agreement may not be modified in any respect other than by a written instrument signed by both parties.

(f) Assignment. This Agreement is not assignable by either party without the other party's written consent.

(g) Interpretation. Any ambiguity in this Agreement shall be resolved to permit compliance by the parties with HIPAA and HITECH.

(h) No Third Party Beneficiary. Nothing in this Agreement is intended, nor shall be deemed, to confer any benefits on any third party.

(i) Severability. In the event that any one or more of the provisions contained in this Agreement shall for any reason be held by a court of competent jurisdiction to be unenforceable in any respect, such holding shall not affect any other provisions of this Agreement, and this Agreement shall then be construed as if such unenforceable provisions are not a part hereof.

In witness whereof, the parties have executed this Agreement as of the Effective Date.

Business Associate	Covered Entity
By:	By:
Name:	Name:
Title:	Title:
Date:	Date: