HIPAA business associate agreement

This Agreement is made between the dental office named below ("Covered Entity") and the vendor named below ("Business Associate"). It sets out how Business Associate may use and must protect protected health information it creates, receives, maintains or transmits for Covered Entity, as required by 45 CFR 164.502(e), 164.504(e), 164.308(b) and 164.314(a).

Covered Entity (office legal name): Office address: Business Associate (legal name):

Business Associate address: Service provided: Underlying service agreement, if any (name and date):

Effective date:

1. Definitions

The following terms used in this Agreement have the same meaning as in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Business Associate has the same meaning as "business associate" at 45 CFR 160.103 and, for this Agreement, means the vendor named above.

Covered Entity has the same meaning as "covered entity" at 45 CFR 160.103 and, for this Agreement, means the dental office named above.

HIPAA Rules means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. Obligations and activities of Business Associate

Business Associate agrees to:

Not use or disclose protected health information other than as permitted or required by this Agreement or as required by law.

Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (the Security Rule) with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by this Agreement.

Report to Covered Entity any use or disclosure of protected health information not provided for by this Agreement of which it 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. Reports are due within the time set in section 7 and in no case later than 60 calendar days after discovery of a breach.

In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information.

Make available protected health information in a designated record set to the party chosen in section 7, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524.

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

Maintain and make available the information required to provide an accounting of disclosures to the party chosen in section 7, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528.

To the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in the performance of those obligations.

Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

3. Permitted uses and disclosures by Business Associate

Business Associate may only use or disclose protected health information as necessary to perform the services described in section 7 or in the underlying service agreement named on page 1.

Business Associate may use or disclose protected health information as required by law.

Business Associate agrees to make uses, disclosures, and requests for protected health information consistent with Covered Entity's minimum necessary policies and procedures.

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 allowed in (e) to (g) below, where they are marked as allowed in section 7.

If allowed in section 7: Business Associate may use protected health information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

If allowed in section 7: Business Associate may disclose protected health information for the proper management and administration of Business Associate or to carry out its legal responsibilities, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be 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.

If allowed in section 7: Business Associate may provide data aggregation services relating to the health care operations of Covered Entity.

4. Covered Entity's duties to inform Business Associate

Covered Entity shall notify Business Associate of any limitation in its notice of privacy practices under 45 CFR 164.520, to the extent the limitation may affect Business Associate's use or disclosure of protected health information.

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 the changes may affect Business Associate's use or disclosure of protected health information.

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 the restriction may affect Business Associate's use or disclosure of protected health information.

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 as allowed in section 3(e) to (g).

5. Term and termination

Term. This Agreement is effective on the effective date on page 1 and ends on the date or event in section 7, or on the date Covered Entity terminates for cause under (b), whichever is sooner.

Termination for cause. Business Associate authorizes termination of this Agreement by Covered Entity if Covered Entity determines that Business Associate has violated a material term of this Agreement and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity.

Obligations of Business Associate upon termination. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity, or, if Covered Entity agrees, destroy, all protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form, and shall retain no copies. If return or destruction is not feasible, Business Associate shall tell Covered Entity why, extend the protections of this Agreement to the information, and limit further uses and disclosures to those purposes that make the return or destruction infeasible, for as long as it keeps the information.

Survival. The obligations of Business Associate under this section survive the termination of this Agreement.

6. Miscellaneous

Regulatory references. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

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.

Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

7. Terms chosen by the parties

Services and permitted purposes (section 3(a))

Describe what Business Associate does for the office that involves protected health information:

Services (for example: hosts our practice management software and backups; IT support for office computers)

Any other permitted purposes

☐ Business Associate may de-identify protected health information under 45 CFR 164.514(a) to (c). Method and allowed uses: _____

Optional uses allowed (section 3(e) to (g))

☐ Use for Business Associate's own management, administration and legal responsibilities (3(e))

☐ Disclosure for those purposes, with the conditions in 3(f)

☐ Data aggregation services for Covered Entity's health care operations (3(g))

☐ None of these

Reporting (section 2(c))

Report unauthorized uses, security incidents and breaches within (days of discovery, 60 or fewer):

Report to (office contact name, email, phone):

☐ Business Associate will send breach notices to individuals, HHS and the media on Covered Entity's behalf, if Covered Entity asks

☐ Covered Entity will send all breach notices itself

Patient requests (sections 2(e) and 2(g))

☐ Business Associate provides access copies and accountings to Covered Entity, within ____ days of the office's request

☐ Business Associate provides them directly to the individual or the individual's designee

☐ Business Associate forwards any request it receives directly from a patient to Covered Entity within ____ days

Term and cure period (section 5)

Agreement ends on (date or event, for example end of service agreement):

Days allowed to cure a material breach before termination:

☐ At termination, Business Associate returns the information to Covered Entity (or to another vendor the office names)

☐ At termination, Business Associate destroys the information and confirms in writing

Signatures

For Covered Entity: name and title

For Business Associate: name and title

Signature and date

Signature and date

Based on the HHS sample business associate agreement provisions and 45 CFR 164.504(e) and 164.314(a). HHS notes that its sample language alone may not be a binding contract under state law and does not replace a lawyer. Have your own lawyer review this agreement. Keep the signed copy for 6 years from the date it was last in effect (45 CFR 164.316(b)(2)(i), 164.530(j)(2)).

Business associate list

complyday.com

Office: Kept by (privacy officer): Last reviewed:

List every vendor that creates, receives, maintains or transmits patient information for the office. Do not write any patient information on this list.

Vendor	Service (what they do with patient information)	Agreement signed (date)	Agreement on file at	Next review

Usually not a business associate (no agreement needed)

Another provider you send information to for treatment, such as an oral surgeon or a dental lab filling your prescription (45 CFR 160.103)

Dental insurance plans you bill for payment

Janitorial, electrical and similar services whose work does not involve patient information, if any access is only incidental and safeguards are in place

The US Postal Service and couriers that only carry information, and banks processing payments

Your own employees and other workforce members