HIPAA Business Associate Agreement

A Lexis Practice Advisor® Practice Note by
Gabriel S. Marinaro, Katten Muchin Rosenman LLP


Gabriel S. Marinaro

FORM SUMMARY

This business associate agreement can be used to satisfy the rule under the Health Insurance Portability and Accountability Act (HIPAA) that requires HIPAA "covered entities" (including many employer-provided group health plans) to enter into a written agreement with any third-party service provider that will handle "protected health information" on behalf of the covered entity (so-called business associates). This form covers the specific business associate agreement requirements under HIPAA's Security and Privacy Rules (see 45 C.F.R. §§ 164.314(a) and 164.504(e)), as amended by Health Information Technology for Economic and Clinical Health Act (HITECH), and includes additional alternate and optional clauses. Based in part on the January 2013 sample agreement available at the Department of Health and Human Services website, this form is enhanced to more clearly reflect HITECH compliance and incorporates numerous drafting notes.

For more information on business associate agreements and HIPAA generally, see HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules.

This Business Associate Agreement (the "Agreement") is entered into between *[name of Covered Entity]* and *[name of Business Associate]* to be effective on *[effective date]* (the "Effective Date").

Drafting Note to First Paragraph

The Business Associate Agreement in the employer-sponsored group health plan context, is typically entered into between the employer's group health plan(s) (as covered entity) and a third-party service provider (the business associate) that is creating, maintaining, or disclosing protected health information. The effective date of the Business Associate Agreement must be effective prior to the disclosure or transmission of PHI to the business associate.

1. **Definitions**

Catch-all definitions:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Breach Notification, Data Aggregation, Designated Record Set, De-Identified Information, Disclosure (Disclose), Electronic Protected Health Information, Electronic Transactions Rule, Enforcement Rule, Genetic Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Sale, Secretary, Security Incident, Security Rule, Subcontractor, Transaction, Unsecured Protected Health Information, and Use.

Specific definitions:

(a)"Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. § 160.103, and in reference to the party to this agreement, shall mean *[name of Business Associate]*.

(b)"Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean *[name of Covered Entity]*.

(c)"HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

(d)"HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act.

2. **Obligations and Activities of Business Associate**

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 C.F.R. 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 it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 C.F.R. § 164.410, and any Security Incident of which it becomes aware;

Drafting Note to Section 2.(c)

The parties may wish to add additional specificity regarding the Breach- and Security Incident-related notification obligations of the Business Associate, such as establishing a specific timeframe and format for the Business Associate to report such incidents, any requirement to report potential Breaches or Security Incidents, and/or whether the Business Associate will have a role in handling Breach Notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media on behalf of the Covered Entity. See also the Breach notification provision in Section 5..

Note that, as a practical matter, Business Associates may not agree to report individually on all Security Incidents of which it becomes aware because that term is broadly defined to include any unauthorized attempted access of the relevant information systems, whether or not successful. A more pragmatic solution is for the Business Associate to promptly report any successful Security Incidents involving Covered Entity protected health information and to provide periodic reports of other Security Incidents on an aggregate basis.

(d)In accordance with 45 C.F.R. §§ 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 *[Covered Entity OR an Individual or Individual's designee]* as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524, including furnishing upon Covered Entity's request or direction an electronic copy of Protected Health Information that is maintained in a Designated Record Set;

Drafting Note to Section 2.(e)

The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for access that the Business Associate receives directly from an Individual (such as whether, and in what time and manner, a Business Associate is to provide the requested access or whether the Business Associate will forward the individual's request to the Covered Entity to fulfill) and the timeframe for the Business Associate to provide information regarding such requests to the Covered Entity so that it can fulfill its documentation obligations.

(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 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526;

Drafting Note to Section 2.(f)

The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for amendment that the Business Associate receives directly from the individual (such as whether and in what time and manner a Business Associate is to act on the request for amendment or whether the Business Associate will forward the individual's request to the Covered Entity) and the timeframe for the Business Associate to incorporate any amendments to the information in the Designated Record Set and to provide information regarding such requests to the Covered Entity so that it can fulfill its documentation obligations.

(g)Maintain and make available the information required to provide an accounting of Disclosures to *[Covered Entity OR an Individual]* as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.

Drafting Note to Section 2.(g)

The parties may wish to add additional specificity regarding how the Business Associate will respond to a request for an accounting of Disclosures that the Business Associate receives directly from the individual (such as whether and in what time and manner the Business Associate is to provide the accounting of Disclosures to the individual or whether the Business Associate will forward the request to the Covered Entity) and the timeframe for the Business Associate to provide information regarding such requests to the Covered Entity so that it can fulfill its documentation obligations.

(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 C.F.R. Part 164 ("Privacy of Individually Identifiable Health Information"), comply with the requirements of such Subpart E that apply to the Covered Entity in the performance of such obligation(s);

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

(j)Not participate in any Sale of Protected Health Information;

(k)Not Use or Disclose Genetic Information for underwriting purposes in violation of the HIPAA Rules;

(l)Comply with the Electronic Transaction Rule and any applicable corresponding requirements adopted by HHS with respect to any Electronic Transactions conducted by Business Associate on behalf of Covered Entity in connection with the services provided under this Agreement.

3. **Representations of Business Associate**

Business Associate agrees that it is directly liable under the HIPAA Rules and the HITECH Act and is subject to civil and, in some cases, criminal penalties for making Uses and Disclosures of Protected Health Information that are not authorized by this Agreement or Required by Law. Business Associate also

acknowledges that it is liable and subject to civil penalties for failing to safeguard Electronic Protected Health Information in accordance with the HIPAA Security Rule.

4. **Permitted Uses and Disclosures by Business Associate**

Business Associate shall not Use or Disclose Protected Health Information relating to Covered Entity, except as expressly permitted under and consistent with this Section 4..

(a)Business Associate may Use or Disclose Protected Health Information for the following permissible purposes: *[list of permissible purposes]*

Drafting Note to Section 4.(a)

List the specific purposes for which protected health information will be used by the Business Associate in its performance of services for the Covered Entity under the Agreement. See Alternate Section 4.(a) for language to set forth this information on a separate schedule. In addition to other permissible purposes, the parties should specify whether the Business Associate is authorized to use protected health information to de-identify the information in accordance with 45 C.F.R. 164.514(a)-(c). The parties also may wish to specify the manner in which the Business Associate will de-identify the information and the permitted uses and disclosures by the Business Associate of the de-identified information.

Alternate Section 4.(a):

(a)

Business Associate may Use or Disclose Protected Health Information as necessary to perform the services set forth in the Service Agreement attached hereto as Exhibit 1.

(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, a copy of which has been furnished to Business Associate.

Drafting Note to Section 4.(c)

See Alternate Section 4.(c) for language to incorporate the Covered Entity's minimum necessary requirements into the business associate agreement in lieu of providing a separate policy and procedures document.

Alternate Section 4.(c):

(c)

Business Associate agrees to make Uses and Disclosures and requests for Protected Health Information subject to the following Minimum Necessary requirements: [include specific provisions that are 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 C.F.R. Part 164 if done by Covered Entity.

Drafting Note to Section 4.(d)

If the Agreement permits the Business Associate to Use or Disclose Protected Health Information for its own management and administration and legal responsibilities or for Data Aggregation services, as set forth in Optional Sections 4.(e), 4.(f), or 4(g) below, then use Alternate Section 4.(d). In such cases, a Covered Entity that wishes to impose specific limitations on these additional permitted uses and disclosures should modify those optional provisions accordingly. See also the optional provisions in Section 5 relating to certain Covered Entity disclosure obligations that may be appropriate for the Business Associate's use of the protected health information.

Alternate Section 4.(d):

(d)

Business Associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except for the specific Uses and Disclosures set forth in the following provisions of this Section 4.

Optional Section 4.(e):

(e)

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.

Optional Section 4.(f):

(e)

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 will notify Business Associate of any instances of which the person becomes aware in which the confidentiality of the information has been Breached.

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

Drafting Note to Section 5.

The optional sections in this Section 5., which impose notification obligations on the Covered Entity, may be appropriate for agreements where the Business Associate is permitted to use the Covered Entity's protected health information for the Business Associate's own purposes (e.g., as provided in Optional Sections 4(e), 4(f), or 4(g)).

Optional Section 5.(a)

(a)

Covered entity shall notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's Use or Disclosure of Protected Health Information.

(b)

Optional Section 5.(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)

Optional Section 5.(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 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's Use or Disclosure of Protected Health Information.

6. **Notification of Breach**

If Business Associate discovers a Breach of Protected Health Information, the Business Associate shall, following the discovery of the Breach of Unsecured Protected Health Information, notify the Covered Entity of such breach in accordance with this Section 6..

(a)A Breach is treated as discovered by Business Associate on the first day on which such breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of Business Associate.

(b)Business Associate shall provide the notification required under this Section 6. without unreasonable delay and in no case later than 60 calendar days after discovery of the Breach.

Drafting Note to Section 6.(b)

The no-reasonable-delay standard with a hard 60-day deadline is the notification timing requirement mandated under HIPAA for Business Associates to alert Covered Entities of a Breach. Covered Entities will often seek to have an earlier timeframe in the business associate agreement.

(c)The notification shall include, to the extent possible, the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach.

(d)Business Associate shall provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual under 45 C.F.R. § 164.404(c) at the time of the notification by Business Associate, and any information that is not then available promptly after such information becomes available. Information to be provided includes, to the extent possible:

(i)A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(ii)A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); and

(iii)A brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches.

Optional Section 7.:

7. **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 C.F.R. Part 164 if done by Covered Entity.

8. **Term and Termination**

(a) Term. The Term of this Agreement shall be effective as of the Effective Date and shall terminate on *[insert termination date or event]* or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity if Covered Entity reasonably determines in good faith that Business Associate has violated a material term of the Agreement.

Drafting Note to Section 8.(b)

This language gives the Covered Entity the discretion to determine whether a violation has occurred that triggers its right to terminate the agreement for cause. Business Associates will often insist on a cure period (see First Alternate Section 8.(b) for sample language). Additionally, Business Associates may seek a reciprocal provision giving them a termination for cause right (see Second Alternate Section 8(b).

First Alternate Section 8.(b):

(b) Termination for Cause.Business Associate authorizes termination of this Agreement by Covered Entity if Covered Entity reasonably determines in good faith that Business Associate has violated a material term of the Agreement and Business Associate has not cured the Breach or ended the violation to the reasonable satisfaction of Covered Entity within [time period] or such longer time period agreed to in writing by Covered Entity.

Second Alternate Section 8.(b):

(b) Termination for Cause.Business Associate authorizes termination of this Agreement by Covered Entity if Covered Entity reasonably determines in good faith that Business Associate has violated a material term of the Agreement and Business Associate has not cured the Breach or ended the violation to the reasonable satisfaction of Covered Entity within [time period] or such longer time period specified by Covered Entity. Covered Entity authorizes termination of this Agreement by Business Associate if Business Associate reasonably determines in good faith that Covered Entity has violated a material term of the Agreement and Covered Entity has not cured the Breach or ended the violation to the reasonable satisfaction of Business Associate within [time period] or such longer time period agreed to in writing by Business Associate.

(c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity (or, if agreed to by Covered Entity, destroy) all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business associate shall retain no copies of the Protected Health Information.

Drafting Note to Section 8.(c)

Use this language if the Business Associate is to return or destroy all Protected Health Information upon termination of the agreement. See Alternate Section 8.(c) if the agreement for language authorizing the Business Associate to retain certain protected health information.

Alternate Section 8.(c):

(c) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, Business Associate, with respect to Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(i)Retain only that Protected Health Information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

(ii)Return to Covered Entity (or, if agreed to by Covered Entity, destroy) the remaining Protected Health Information that the Business Associate still maintains in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Electronic Protected Health Information to prevent Use or Disclosure of the Protected Health Information, other than as provided for in this Section, for as long as Business Associate retains the Protected Health Information;

(iv) Not Use or Disclose the Protected Health Information retained by Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out at [Section 4(e) AND/OR Section 4(f)] which applied prior to termination; and

(v) Return to Covered Entity (or, if agreed to by Covered Entity, destroy) the Protected Health Information 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.

Optional Section 8.(d):

(d)

If so directed by Covered Entity, Business Associate will transmit any Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, to another Business Associate of Covered Entity at termination.

Optional Section 8.(e):

(d)
Business Associate shall be responsible for compliance with the obligations described in Section 8.(c) with respect to any applicable Protected Health Information created, received, or maintained by Subcontractors of the Business Associate.

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

Optional Section 9.:

9. **Indemnification**
[Insert indemnification language agreed to by the parties.]

10. **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. Any amendment to this Agreement must be in writing and signed by both parties.

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

(d) Governing law.This Agreement shall be governed by the laws of *[state]*, except to the extent preempted by federal law.

(e) Counterparts.This Agreement may be executed in any number of counterparts, and may be signed via facsimile or e-mail (scan), and each such counterpart shall be deemed to be an original instrument, but all such counterparts shall constitute one agreement.

(f) Severability.The provisions of this Agreement shall be severable, and the invalidity of any provision shall not affect the validity of other provisions.

(g) Entire Agreement.This Agreement contains the entire agreement between the parties. This Agreement supersedes all prior agreements, understandings or writings, whether oral or written with regard to this subject matter.

(h) Notice.Any notice required under this Agreement shall be in writing and shall be given by (i) delivery in person, (ii) by a nationally recognized next day courier service, (iii) by first class, registered or certified mail, postage prepaid, (iv) by electronic mail to the address of the party specified in this Agreement or such other address as either party may specify in writing.

Drafting Note to Section 10.

The miscellaneous provisions provided here are fairly commonplace, but they are not mandatory for business associate agreements to comply with HIPAA requirements.

Gabriel S. Marinaro
Special Counsel, Katten Muchin Rosenman LLP

Gabriel Marinaro serves as special counsel in the Employee Benefits and Executive Compensation group. His practice focuses on all aspects of employee benefits and executive compensation. He regularly counsels publicly traded and privately held companies, tax-exempt organizations, and governmental entities on a variety of employee benefits and executive compensation matters. Gabe regularly advises both employers and executives on a wide range of executive compensation matters, including drafting employment agreements, equity compensation arrangements, severance agreements and bonus plans. Gabe provides guidance on nonqualified deferred compensation plans both for for-profit companies and tax-exempt clients. Gabe regularly drafts nonqualified deferred compensation arrangements, including supplemental executive retirement plans, and change in control agreements. Additionally, Gabe advises employers and executives on issues under Code Sections 409A, 457(f), 457A, 162(m), 280G and 83 regarding compensation arrangements for executives.

Gabe assists both publicly traded and privately held companies with equity compensation matters, including drafting equity incentive plans, securities filings, award agreements, and other documentation surrounding the implementation of an equity incentive plan and the underlying awards. Gabe also has drafted and advised on profits interests plans and unit appreciation rights plans for limited liability companies.