

Google Apps HIPAA Business Associate Amendment

This HIPAA Business Associate Amendment (“HIPAA BAA”) is made and entered into by and between Google Inc. and Customer effective as of the date electronically accepted by Customer and amends the Agreement for the purpose of implementing the requirements of HIPAA to support the parties’ compliance requirements thereunder. The “Agreement” refers to the Google Apps for Work (or Business), Education, or Government Agreement entered into between the parties pursuant to which Google Inc. provides Services to Customer. Customer must have an existing Agreement in place for this HIPAA BAA to be valid and effective. Together with the Agreement, this HIPAA BAA will govern each party’s respective obligations regarding Protected Health Information (defined below).

You represent and warrant that: (i) you have full legal authority to bind Customer to this HIPAA BAA, (ii) you have read and understand this HIPAA BAA, and (iii) you agree, on behalf of Customer, to the terms of this HIPAA BAA. If you do not have legal authority to bind Customer, or do not agree to these terms, please do not sign or accept the terms of this HIPAA BAA.

The parties agree as follows:

1. **Definitions.** For purposes of this HIPAA BAA, any capitalized terms not otherwise defined herein will have the meaning given to them in the Agreement and under HIPAA.

“Google” means Google Inc. and its affiliates that provide the Services.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended (including with respect to the HITECH Act).

“HIPAA Implementation Guide” means the informational guide that Google makes available describing how Customer can configure and use the Services to support HIPAA compliance. The HIPAA Implementation Guide is available for review at the following URL:

https://static.googleusercontent.com/media/www.google.com/en/us/work/apps/terms/2015/1/hipaa_implementation_guide.pdf (as the content at that URL, or such other URL as Google may provide, may be updated by Google from time to time)

“HITECH Act” means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

“Included Functionality” means functionality within the Services as described at the following URL: www.google.com/work/apps/terms/2015/1/hipaa_functionality.html (as the content at that URL, or such other URL as Google may provide, may be updated by Google from time to time).

“Protected Health Information” or “PHI” will have the meaning given to it under HIPAA to if provided to Google as Customer Data in connection with Customer’s permitted use of Included Functionality.

“Security Rule” means 45 C.F.R., Part 164, Subpart C, under HIPAA.

“Services” means the Google Apps Core Services as defined under the applicable Agreement.

2. Applicability.

a. Parties. This HIPAA BAA applies to the extent Customer is acting as a Covered Entity or Business Associate, to create, receive, maintain or transmit PHI via the Included Functionality and where Google, as a result, is deemed under HIPAA to be acting as a Business Associate of Customer.

b. Services Scope. As of the effective date of this Amendment, this Amendment is applicable only to the Included Functionality. Google may expand the scope of Included Functionality. If Google expands the scope of Included Functionality then this HIPAA BAA will automatically apply to such additional new functionality and features as of the date the Included Functionality description is updated, or the date Google has otherwise provided written communication regarding an update to the scope of Included Functionality to Customer’s Notification Email Address (whichever date is earlier).

3. Permitted Use and Disclosure.

- a. By Google. Google may use and disclose PHI only as permitted under HIPAA as specified in the Agreement and under this HIPAA BAA. Google may also use and disclose PHI for the proper management and administration of Google’s business and to carry out the legal responsibilities of Google, provided that any disclosure of PHI for such purpose may only occur if: (1) required by applicable law; or (2) Google obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Google will be notified of any Breach.
- b. By Customer. Customer will not request Google or the Services to use or disclose PHI in any manner that would not be permissible under HIPAA if done by a Covered Entity itself (unless otherwise expressly permitted under HIPAA for a Business Associate). In connection with Customer’s management and administration of the Services to End Users, Customer is responsible for using the available controls within the Services to support its HIPAA compliance requirements, including reviewing the HIPAA Implementation Guide and enforcing appropriate controls to support Customer’s HIPAA compliance. Customer will not use the Services to create, receive, maintain or transmit PHI to other Google services outside of the Included Functionality, except where Google has expressly entered into a separate HIPAA business associate agreement for use of such Google services. If Customer uses Included Functionality in connection with PHI, Customer will use controls available within the Services to ensure: (i) all other Google products not part of the Services are disabled for all End Users who use Included Functionality in connection with PHI (except those services where Customer and Google already have an appropriate HIPAA business associate agreement in place); and (ii) it takes appropriate measures to limit its use of PHI in the Services to the minimum

extent necessary for Customer to carry out its authorized use of such PHI. Customer agrees that Google has no obligation to protect PHI under this HIPAA BAA to the extent Customer creates, receives, maintains, or transmits such PHI outside of the Included Functionality (including Customer's use of its offline or on-premise storage tools or third party applications).

4. **Appropriate Safeguards.** Google and Customer will use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, consistent with this HIPAA BAA, and as otherwise required under the Security Rule, with respect to the Included Functionality.
5. **Reporting.** Google will promptly notify Customer following the discovery of a Breach resulting in the unauthorized use or disclosure of PHI in violation of this HIPAA BAA in the most expedient time possible under the circumstances, consistent with the legitimate needs of applicable law enforcement and applicable laws, and after taking any measures necessary to determine the scope of the Breach and to restore the reasonable integrity of the Services system by using commercially reasonable efforts to mitigate any further harmful effects to the extent practicable. Google will send any applicable Breach notifications to the Notification Email Address (as such contact is designated in the Services by Customer) or via direct communication with the Customer. For clarity, Customer and not Google, is responsible for managing whether its End Users are authorized to create, receive, maintain or transmit PHI within the Services and Google will have no obligations relating thereto. This Section 5 will be deemed as notice to Customer that Google periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification or destruction of information or interference with the general operation of Google's information systems and the Services and even if such events are defined as a Security Incident under HIPAA, Google will not provide any further notice regarding such unsuccessful attempts.
6. **Agents and Subcontractors.** Google will take appropriate measures to ensure that any agents and subcontractors used by Google to perform its obligations under the Agreement that require access to PHI on behalf of Google are bound by written obligations that provide the same material level of protection for PHI as this HIPAA BAA. To the extent Google uses agents and subcontractors in its performance of obligations hereunder, Google will remain responsible for their performance as if performed by Google itself under the Agreement.
7. **Accounting Rights.** Google will make available to Customer the PHI via the Services so Customer may fulfill its obligation to give individuals their rights of access, amendment, and accounting in accordance with the requirements under HIPAA. Customer is responsible for managing its use of the Services to appropriately respond to such individual requests.
8. **Access to Records.** To the extent required by law, and subject to applicable attorney client privileges, Google will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Google on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this HIPAA BAA.
9. **Return/Destruction of Information.** Google agrees that upon termination of the Agreement, Google will return or destroy all PHI received from Customer, or created or

received by Google on behalf of Customer, which Google still maintains in accordance with the section titled "Effects of Termination" (or as otherwise expressly agreed in writing) under the Agreement; provided, however, that if such return or destruction is not feasible, Google will extend the protections of this HIPAA BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. In the event this HIPAA BAA is terminated earlier than the underlying Agreement Customer may continue to use the Services in accordance with the Agreement, but must delete any PHI it maintains in the Services and cease to create, receive, maintain or transmit such PHI to Google or within the Services.

10. **Breach/Cure.** Customer may immediately terminate this HIPAA BAA and the Agreement upon 10 days written notice to Google if Google has materially breached this HIPAA BAA and such breach is not reasonably capable of being cured.
11. **Term.** This HIPAA BAA will expire upon the earlier of: (i) a permitted termination in accordance with this HIPAA BAA; (ii) the natural expiration or termination of the existing Agreement; or (ii) the execution of an updated HIPAA BAA that supersedes this HIPAA BAA.
12. **Interpretation.** It is the parties' intent that any ambiguity under this HIPAA BAA be interpreted consistently with the intent to comply with applicable laws.
13. **Effect of Amendment.** This HIPAA BAA supersedes in its entirety any pre-existing HIPAA BAA executed by the parties covering the same Services. To the extent of any conflict or inconsistency between the terms of this HIPAA BAA and the remainder of the Agreement, the terms of this HIPAA BAA will govern. Except as expressly modified or amended under this HIPAA BAA, the terms of the Agreement remain in full force and effect. By Customer electronically accepting or signing the terms of this HIPAA BAA made available by Google, Customer and Google (on behalf of itself and its affiliates that provide the Services) agree that it constitutes a written agreement between the parties.

Agreed and accepted by the parties as of the signature date below.

Google Apps Domain Name:

Customer:
(Company / Institution / Organization)

By:

Name:

Title:

Email:

Date: