



## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”), effective on the date set forth below (“Effective Date”), is entered into by and between the GoTo Group of entities, including all direct and indirect subsidiaries and affiliates that are controlled by or are under common control with GoTo Group, Inc. (“Business Associate”), and the “Covered Entity” identified below, on behalf of itself and its majority owned or controlled subsidiaries (“Covered Entity”) (each a “Party” and collectively the “Parties”).

WHEREAS, GoTo is a provider of a suite of on-line, cloud-based, Software-as-a-Service solutions (each a “Service”), which are hosted by GoTo from within its own data center servers, and may be accessed by its customers on-demand, over the Internet; and

WHEREAS, Business Associate licenses its Service to Covered Entity as memorialized in a separate agreement (the “Underlying Agreement”); and

WHEREAS, the Covered Entity intends to use the Service in a way that may result in the disclosure and processing of certain Protected Health Information (“PHI”) through the Service and the data centers used by GoTo to provide the Service; and

WHEREAS, despite the fact that GoTo does **not** require routine access to any PHI to provide the Service, to the extent applicable, the Parties are committed to complying with the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E as amended from time to time (the “Privacy Rule”), and with the Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C as amended from time to time (the “Security Rule”), under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act and its implementing regulations (“HITECH”).

NOW, THEREFORE, this Agreement sets forth the terms and conditions pursuant to which PHI, and, when applicable, Electronic Protected Health Information (“ePHI”), shall be handled. The Parties agree as follows:

### 1. Definitions

1.1 **General Definitions.** All terms appearing in this BAA with initial upper case letters that are not otherwise defined in this Agreement have the same meaning as that provided for the respective terms in 45 C.F.R. §§ 160.103, 164.103, 164.304, 164.402, and 164.501, whichever is applicable. To the extent any conflicts exist between the meanings assigned to the respective terms in this BAA and HIPAA, the HIPAA meanings control for purposes of this Agreement.

1.2 **Specific Definitions.** For purposes of this BAA, the following terms have the indicated meanings whenever the term appears with initial upper case letters:

1.2.1 **“Breach”** means the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by HIPAA which compromises the security or privacy of the Protected Health Information unless such acquisition, access, use or disclosure is otherwise excluded under 45 C.F.R. § 164.402.

1.2.2 **“Covered Entity”** means the same as the term is defined in 45 C.F.R. § 164.103.

1.2.3 **“Data Aggregation”** means, with respect to Protected Health Information created or received by GoTo in its capacity as the Business Associate of the Covered Entity, the combining of such Protected Health Information by GoTo with the Protected Health Information received by GoTo in its capacity as Business Associate of another covered entity, to permit data analyses that relate to the health care operations of the respective entities.

1.2.4 **“Designated Record Set”** means a group of records maintained by or for Covered Entity within the meaning of 45 C.F.R. § 164.501 that consists of: (i) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (ii) records that are used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. For purposes of this section, the term “record” means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for the Covered Entity.

1.2.5 **“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as amended.

1.2.6 **“HITECH”** means the Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5.

1.2.7 **“Individual”** has the same meaning as the term “individual” in 45 C.F.R. § 160.103, and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

- 1.2.8 **"Privacy Rule"** means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and E.
- 1.2.9 **"Protected Health Information"** or "PHI" means individually identifiable health information that is transmitted by electronic media (within the meaning of 45 C.F.R. § 160.103), maintained in electronic media, or maintained or transmitted in any form or medium that are received by GoTo from or on behalf of the Covered Entity in connection with the performance of Services, and relates to:
- (a) The past, present or future physical or mental health or condition of an Individual;
  - (b) The provision of health care to an Individual; or
  - (c) The past, present or future payment for the provision of health care to an Individual;
- and that identifies or could reasonably be used to identify an individual, and otherwise has the meaning given to that term under the Privacy Rule including, but not limited to, 45 C.F.R. § 160.103. Protected Health Information does **not** include health information that has been de-identified in accordance with the standards for de-identification provided for in the Privacy Rule including 45 C.F.R. § 164.514 or Individually Identifiable Health Information: (i) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a Covered Entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.
- 1.2.10 **"Required by Law"** has the same meaning as the term "Required by Law" in 45 C.F.R. § 164.103.
- 1.2.11 **"Secretary"** means the Secretary of the United States Department of Health and Human Services ("HHS") or his designee.
- 1.2.12 **"Security Rule"** means the Security Standards at 45 C.F.R. Part 160, Part 162, and Part 164.
- 1.2.13 **"Services"** means the functions, activities or services to be provided to Covered Entity under the terms of the Agreement.

## 2. Permitted Uses and Disclosures of PHI

- 2.1 GoTo may use or disclose PHI only as permitted or required by this Business Associate Agreement or as Required by Law.
- 2.2 GoTo may use and disclose PHI that it receives on Covered Entity's behalf or receives directly from Covered Entity, and to request PHI on Covered Entity's behalf (collectively, "Covered Entity's PHI") to perform its obligations under the Agreement, for the proper management and administration of GoTo's business, and to otherwise carry out its legal responsibilities in a manner permitted by applicable law.
- 2.3 GoTo may disclose PHI if the disclosure is Required by Law. GoTo may also disclose PHI for the proper management and administration of the business of GoTo, provided GoTo obtains reasonable assurances from the person to whom the information is disclosed that (i) such PHI will be held confidentially and used or further disclosed only as Required by Law and for the purpose for which such PHI was disclosed, and (ii) such person will notify GoTo of any instances in which such person becomes aware of any breaches to the confidentiality of that PHI.
- 2.4 Covered Entity agrees to disclose to GoTo only the minimum amount of PHI reasonably necessary to accomplish the intended purpose of use under the Agreement. For clarity, de-identified information does not constitute PHI, and is not subject to the terms of this Agreement.

## 3. Safeguards and Subcontracting

- 3.1 GoTo agrees to maintain appropriate safeguards including administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI in accordance with Subpart C of the Security Rule (45 C.F.R. § 164) to prevent use or disclosure of such PHI other than as provided in this Agreement.
- 3.2 With respect to any Subcontractor or agent to whom GoTo provides PHI, GoTo will first contractually obligate that Subcontractor or agent to agree to protect PHI pursuant to terms and conditions at least as protective as the terms of this Agreement and in compliance with the applicable requirements of Subpart C of the Security Rule.

## 4. Unauthorized Use and Disclosure

- 4.1 GoTo will promptly notify Covered Entity of the following events to the extent it becomes aware of (1) any Breach of unsecured PHI; or (2) any "Security Incident" as the term is defined in 45 C.F.R. § 164.304, each of the foregoing (1)-(2) only as applicable to information GoTo creates, receives, maintains or transmits from or on behalf of Covered Entity. Notwithstanding these assurances, the Parties acknowledge and agree that this section constitutes notice by GoTo to Covered Entity of the ongoing existence and occurrence of attempted but "Unsuccessful Security Incidents" for which no additional notice to Covered Entity is required. "Unsuccessful Security Incidents" includes pings and other broadcast attacks on GoTo's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no successful security incident results in unauthorized access, use or disclosure of PHI.
- 4.2 If applicable, and to the extent possible, GoTo's notice to Covered Entity under this section will include the content set out in 45 C.F.R. § 164.410, including the following information: (a) the date of discovery of the Breach; (b) the identification of individuals and/or classes of individuals who are subject to the Breach; and (3) a general description of the nature of the Breach. To the extent GoTo is responsible for a Breach, and subject to any limitations of liability set forth herein, GoTo will use reasonable efforts to mitigate, to the extent practicable, any

harmful effect arising from that Breach. The Parties agree to cooperate when making any required notifications to the affected Individuals with respect to any such Breach.

## **5. Designated Record Sets**

5.1 Unless otherwise explicitly stated in the Agreement, the Parties do not intend for GoTo to maintain any PHI in a Designated Record Set for the Covered Entity. The Covered Entity agrees to provide GoTo only copies of PHI, and to retain all original documents, so that GoTo maintains no unique records in any Designated Record Set.

5.2 To the extent GoTo maintains a Designated Record Set on behalf of the Covered Entity, and to the extent GoTo maintains the only copy of PHI, GoTo agrees as follows:

5.2.1 GoTo shall provide access, at the written request of Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual to meet the requirements under 45 C.F.R. Section 164.524.

5.2.2 Upon receipt of a written request by Covered Entity, to the extent technically practicable, GoTo shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to, pursuant to 45 C.F.R. Section 164.526.

## **6. Covered Entity Obligations**

6.1 Covered Entity will notify GoTo of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. Section 164.520, to the extent that this limitation may affect GoTo's use or disclosure of PHI in accordance with this Agreement. GoTo agrees to make commercially reasonable efforts to comply with such limitations communicated by Covered Entity.

6.2 Covered Entity will notify GoTo of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect GoTo's use or disclosure of PHI in accordance with this Agreement. GoTo agrees to comply with those changes in, or revocation of, permission communicated by Covered Entity, to the extent practicable under the Agreement.

6.3 Covered Entity will notify GoTo of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. Section 164.522, to the extent that those restrictions may affect GoTo's use or disclosure of PHI in accordance with this Agreement. GoTo shall comply with any restrictions communicated by Covered Entity, to the extent practicable under the Agreement and applicable law.

6.4 Covered Entity is responsible for using the available controls within the Services to support its HIPAA compliance.

## **7. Compliance with Law**

7.1 Each Party is responsible for its own compliance with any and all existing or subsequent laws, whether by statute, regulation, common law, or otherwise, related to its acquisition, access, use or disclosure of PHI. Covered Entity agrees that it shall have and maintain appropriate consents from data subjects, as may be necessary and Required by Law, for GoTo to acquire, access, use or disclose PHI in accordance with its delivery of services under the Agreement and as otherwise permitted under this Agreement.

7.2 Upon request by the HHS, GoTo will make available to HHS the internal practices, books, and records of GoTo relating to the use and disclosure of PHI for purposes of ensuring compliance with the provisions of HIPAA.

7.3 In the event that GoTo receives an inquiry from an individual for access to or the right to amend PHI, it shall advise Covered Entity of that communication and the request. The Parties agree to cooperate in making PHI available to the individual and in making the requested amendment of PHI. Covered Entity retains and will make available on request information required to provide an accounting of disclosures in accordance with the provisions of HIPAA.

## **8. Miscellaneous**

8.1 Term. This Agreement shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Agreement. Certain provisions and requirements of this Agreement shall survive its expiration or other termination as set forth in Section 8.5.

8.2 Termination. Either Covered Entity or GoTo may terminate this Agreement and any related agreements if the terminating Party determines in good faith that the terminated Party has breached a material term of this Agreement; provided, however, that no Party may terminate this Agreement if the breaching Party cures such breach to the reasonable satisfaction of the non-breaching Party within thirty (30) business days after the breaching Party's receipt of written notice of such breach.

8.3 Automatic Termination. This Agreement shall automatically terminate without any further action of the Parties upon the termination or expiration of GoTo's provision of Service(s) to Covered Entity.

8.4 Effect of Termination. Upon termination or expiration of this Agreement for any reason, GoTo shall, upon the written request of Covered Entity, return or certify that it has destroyed all PHI pursuant to 45 C.F.R. § 164.504(e)(2)(ii)(J) if, and to the extent that, it is reasonably feasible to do so. Prior to doing so, GoTo shall recover any PHI in the possession of its subcontractors or agents. To the extent it is not feasible for GoTo to return or destroy any portion of the PHI, GoTo shall provide Covered Entity a statement that GoTo has determined that

it is infeasible to return or destroy all or some portion of the PHI in its possession or in possession of its subcontractors or agents. GoTo shall extend any and all protections, limitations and restrictions contained in this Agreement to any PHI retained after the termination of this Agreement until such time as the PHI is returned to Covered Entity or destroyed.

- 8.5 Survival. The respective rights and obligations of GoTo and Covered Entity under the provisions of Sections 8.4, 8.5 and 8.9, and Section 2 (solely with respect to PHI that GoTo retains in accordance with Section 8.4 because it is not feasible to return or destroy such PHI), shall survive termination of this Agreement until such time as the PHI is returned to Covered Entity or destroyed. In addition, Section 5 shall survive termination of this Agreement, provided that Covered Entity determines that the PHI being retained pursuant to Section 8.4 constitutes a Designated Record Set.
- 8.6 Amendments; Waiver. This Agreement may not be modified or amended, except in a writing duly signed by authorized representatives of the Parties. To the extent that any relevant provision of the HIPAA or HITECH is materially amended in a manner that changes the obligations of GoTo or Covered Entities, the Parties agree to negotiate in good faith appropriate amendment(s) to this Agreement to give effect to the revised obligations. Further, no provision of this Agreement shall be waived, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.
- 8.7 Integration. This Agreement is the sole and complete agreement between the Parties relating to obligations under HIPAA and HITECH, and supersedes any prior agreements, understandings, and communications relating thereto. Notwithstanding the foregoing, the Underlying Agreement(s) shall govern all other terms between the Parties including, without limitation, terms related to the Services provided, payment obligations, and liability with respect to both the Underlying Agreement(s) and this Business Associate Agreement.
- 8.8 No Third-Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.
- 8.9 Notices. Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to such Party's address given below, and/or via facsimile to the facsimile telephone numbers listed below. Each Party may change its address and that of its representative for notice by the giving of notice thereof in the manner provided. Such notice is effective upon receipt of notice, but receipt is deemed to occur on next business day if notice is sent by FedEx or other overnight delivery service.
- 8.10 Counterparts; Facsimiles. This Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.
- 8.11 Choice of Law; Interpretation. This Agreement shall be governed by the laws of the Commonwealth of Massachusetts; as provided, however, that any ambiguities in this Agreement shall be resolved in a manner that allows GoTo to comply with the Privacy Rule, and, if applicable, the Security Rule.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf as of the Effective Date.

**GOTO GROUP, INC.**

**COVERED ENTITY:** \_\_\_\_\_

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: Claire Bergen

Name: \_\_\_\_\_

Title: Associate General Counsel

Title: \_\_\_\_\_

Date:

**Effective Date:** \_\_\_\_\_

**Notice Address:** Attn: Legal Department

**Notice Address:** Attn: Legal Department

Address: 333 Summer Street,  
Boston, Massachusetts 02210 USA

Address: \_\_\_\_\_

Email: [legal@goto.com](mailto:legal@goto.com)

Email: \_\_\_\_\_

Tel: 1-781-638-9094

Tel: \_\_\_\_\_

Fax: 1-781-998-2597

Fax: \_\_\_\_\_