BUSINESS ASSOCIATE AGREEMENT

EXPLANATORY NOTE

Ottoclip's standard Business Associate Agreement for healthcare customers. We recommend that healthcare customers record only on a test account with fake patient data, ideally on a staging copy of their product, meaning a test copy kept apart from the one real patients' records live in. Then no patient information reaches Ottoclip, and your own counsel may find that no BAA is needed. When your policy still requires one, Ottoclip signs this agreement with Business and Enterprise customers. To start, email legal@ottoclip.com. This note explains the agreement and is not part of it.

This Business Associate Agreement ("**BAA**") is made as of [Effective Date] (the "**Effective Date**") between CollectiveSoft, Inc., doing business as Ottoclip ("**Ottoclip**"), and [Customer legal name] ("**Customer**").

BACKGROUND

Customer uses the Ottoclip service under [the Ottoclip Terms of Service / the order form dated ___] (the "**Agreement**"). Customer is a Covered Entity under HIPAA, or a business associate of one or more Covered Entities. Customer uses Ottoclip to record flows in Customer's web product, and Ottoclip turns them into narrated videos, interactive demos, guided walkthroughs, static guides, and animations. While doing that, Ottoclip may create, receive, keep, or send Protected Health Information on Customer's behalf. When Customer is itself a business associate, Ottoclip is its subcontractor, and this BAA is the subcontractor agreement HIPAA requires. This BAA sets the terms for handling that information so that both parties meet HIPAA.

1. DEFINITIONS

1.1 A capitalized term this BAA does not define has the meaning the HIPAA Rules give it. These include Breach, Covered Entity, Designated Record Set, Disclosure, Individual, Minimum Necessary, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1.2 "**HIPAA Rules**" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and 164, as amended, including by the HITECH Act.

1.3 "**Customer PHI**" means Protected Health Information, as defined at 45 C.F.R. 160.103, that Ottoclip creates, receives, keeps, or sends on Customer's behalf through the Services. It includes electronic Protected Health Information.

1.4 "**Services**" means the services Ottoclip provides to Customer under the Agreement, as listed in Exhibit A.

1.5 "**Approved Environments**" means the web addresses listed in Exhibit A where Customer may record flows and set content to regenerate.

2. HOW CUSTOMER PHI CAN REACH OTTOCLIP

Both parties agree the Services handle Customer's data in the following ways, so either party can tell where Customer PHI may be held.

(a) While a user records a flow, the Ottoclip browser extension captures the pages visited, the text shown on them, the values typed into fields, the page addresses, and a video of the browser tab.

(b) To generate and regenerate content, Ottoclip opens Customer's product in a browser on Ottoclip's own computers, replays the recorded steps, and captures screenshots, video, and a log of each run that can include page text. Customer can set this to run on a schedule.

(c) Recordings, scripts, screenshots, videos, and generated content are stored in Ottoclip's database and cloud storage. Ottoclip sends parts of them to the Subcontractors in Exhibit B to write narration and build content.

(d) Recordings and content travel between browsers and Ottoclip over encrypted connections through the network providers in Exhibit B.

(e) Ottoclip hosts the generated content at links and embeds that Customer shares.

(f) When Customer asks for help, Ottoclip staff may open Customer's product and content to set up or repair a script.

Any Protected Health Information shown in Customer's product during any of these steps can become Customer PHI. This list describes how the Services work. It does not limit Ottoclip's duties for Customer PHI held anywhere else.

3. WHAT OTTOCLIP MAY DO WITH CUSTOMER PHI

3.1 Ottoclip may use and disclose Customer PHI only to provide the Services to Customer, as this BAA allows, or as Required by Law.

3.2 Ottoclip may use Customer PHI for its proper management and administration and to carry out its legal duties. It may disclose Customer PHI for those purposes only when the disclosure is Required by Law, or when Ottoclip first gets written assurance from the recipient of three things. The recipient will keep the information confidential. It will use or disclose it further only as Required by Law or for the purpose Ottoclip disclosed it for. It will tell Ottoclip of any case it knows of where the information's confidentiality was breached.

3.3 Ottoclip will not use or disclose Customer PHI in a way that would break Subpart E of 45 C.F.R. Part 164 if Customer did it, except as Section 3.2 allows.

3.4 Ottoclip will not use Customer PHI to train, test, or improve any AI model, or to develop or improve Ottoclip's products. Ottoclip will not copy Customer PHI into test data or into any system it uses to build or test its software. Ottoclip will not de-identify Customer PHI for its own use, combine it with other customers' data, sell it, or use it for marketing. Setting up and repairing Customer's scripts, and fixing faults in the Services that affect Customer, are part of providing the Services.

3.5 Ottoclip will limit its uses, disclosures, and requests of Customer PHI to the Minimum Necessary.

4. OTTOCLIP'S DUTIES

4.1 Safeguards. Ottoclip will use appropriate administrative, physical, and technical safeguards, and will comply with Subpart C of 45 C.F.R. Part 164 for electronic Customer PHI, to prevent any use or disclosure this BAA does not allow. These safeguards include the following.

(a) Customer PHI is encrypted while it travels over public networks and while it is stored.

(b) Stored recordings, screenshots, and scripts are never reachable at a public address. Only generated content that Customer chooses to share is.

(c) Only named Ottoclip staff who need access to provide the Services can reach Customer PHI, each with their own login, and access to stored Customer PHI is logged.

(d) Computers that hold Customer PHI, including the computers that generate content, use full-disk encryption, lock when left idle, and are kept in known locations.

(e) Staff who can reach Customer PHI are trained on HIPAA and on this BAA, and face sanctions for breaking either.

(f) Ottoclip keeps a written security risk analysis and reviews it at least once a year.

4.2 Reporting. Ottoclip will report the following to Customer in writing.

(a) Any use or disclosure of Customer PHI that this BAA does not allow, within 10 business days after Ottoclip discovers it.

(b) Any Security Incident involving Customer PHI, within 10 business days after Ottoclip discovers it.

(c) Any Breach of Unsecured Protected Health Information, without unreasonable delay and no later than 10 business days after Ottoclip discovers it, as 45 C.F.R. 164.410 defines discovery. To the extent Ottoclip knows them, the report will name each Individual affected and describe what happened, when it happened and when it was discovered, the kinds of

information involved, and what Ottoclip has done to look into it, limit harm, and prevent it happening again. It will also include anything else Customer needs to give its own notices under 45 C.F.R. 164.404. Ottoclip will add to the report as it learns more.

This section is Ottoclip's notice to Customer of attempted Security Incidents that do not succeed, and no further report of them is needed. These include pings, port scans, failed sign-in attempts, denial-of-service attempts, and similar events that do not lead to unauthorized access to, or use, disclosure, change, or destruction of, Customer PHI.

Customer decides whether a Breach must be reported to Individuals, the Secretary, the media, or a Covered Entity that Customer serves, and Customer sends those notices. Ottoclip will not send them unless Customer asks in writing or the law requires it.

4.3 Limiting harm. Ottoclip will take reasonable steps to limit any harmful effect it knows of from a use or disclosure of Customer PHI that breaks this BAA.

4.4 Subcontractors. As 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2) require, Ottoclip will make sure every Subcontractor that creates, receives, keeps, or sends Customer PHI for Ottoclip agrees in writing to substantially the same restrictions and conditions on Customer PHI that apply to Ottoclip under this BAA. Exhibit B lists these Subcontractors. Ottoclip will give Customer at least 30 days' written notice before a new Subcontractor receives Customer PHI. If Customer objects in writing during that time and the parties cannot settle the objection, Customer may end the affected Services and receive a refund of fees prepaid for the time after they end. Ottoclip may stop using a Subcontractor at any time, and will update Exhibit B when it adds or removes one.

4.5 Access. If Ottoclip keeps Customer PHI in a Designated Record Set, it will make that information available to Customer within 15 days of Customer's request, so Customer can meet 45 C.F.R. 164.524.

4.6 Amendment. If Ottoclip keeps Customer PHI in a Designated Record Set, it will make the changes Customer directs within 15 days of Customer's request, so Customer can meet 45 C.F.R. 164.526.

4.7 Accounting of disclosures. Ottoclip will record the disclosures of Customer PHI that Customer would need to account for under 45 C.F.R. 164.528, including the date of each disclosure, who received it, what was disclosed, and why. Ottoclip will give that record to Customer within 15 days of Customer's request.

4.8 Requests from individuals. If an Individual asks Ottoclip directly for access, an amendment, or an accounting, Ottoclip will send the request to Customer within 5 business days and will not answer it unless Customer directs it to.

4.9 Carrying out Customer's duties. If Ottoclip carries out any duty of Customer under Subpart E of 45 C.F.R. Part 164, Ottoclip will meet the requirements of Subpart E that apply to that duty.

4.10 Books and records. Ottoclip will make its internal practices, books, and records about Customer PHI available to the Secretary for the purpose of deciding whether Customer and Ottoclip comply with the HIPAA Rules. Unless the law forbids it, Ottoclip will tell Customer promptly of any such request.

4.11 Location. Ottoclip will store Customer PHI only in the United States, and will send it only to Subcontractors that store and process it in the United States.

4.12 Real patient data. Ottoclip staff will open Customer's product only in the Approved Environments. If Ottoclip learns that a recording, a replay, or generated content holds information about a real patient, it will tell Customer, and it may pause scheduled regeneration of the affected content until Customer fixes the cause. Ottoclip will delete that information within 10 business days after Customer asks.

5. CUSTOMER'S DUTIES

5.1 Customer will tell Ottoclip in writing of the following, to the extent each affects how Ottoclip may use or disclose Customer PHI.

(a) Any limit in Customer's notice of privacy practices, or in the notice of the Covered Entity Customer serves.

(b) Any change to, or withdrawal of, an Individual's permission to use or disclose their information.

(c) Any restriction Customer has agreed to under 45 C.F.R. 164.522.

5.2 Customer will not ask Ottoclip to use or disclose Customer PHI in a way that Subpart E of 45 C.F.R. Part 164 would not allow Customer to, except as Section 3.2 allows.

5.3 To keep the Customer PHI that reaches Ottoclip to the Minimum Necessary, Customer will do the following.

(a) Record flows, and set content to regenerate, only in the Approved Environments.

(b) Use only demo, test, or de-identified data in the Approved Environments, as Exhibit A describes. De-identified means de-identified under 45 C.F.R. 164.514(b).

(c) Tell Ottoclip promptly if it learns that real patient information was shown during a recording or a replay, so Ottoclip can delete it.

(d) Keep Protected Health Information out of the narration, step names, notes, support requests, and other text Customer types into or sends to Ottoclip.

(e) Set any generated content that shows Protected Health Information to require sign-in before it can be viewed.

5.4 Content that Customer chooses to share on a public link or embed, or downloads and sends elsewhere, is a disclosure made by Customer and not by Ottoclip.

5.5 Customer is responsible for having any permission HIPAA requires before it makes Customer PHI available to Ottoclip.

5.6 Customer PHI that reaches Ottoclip from outside the Approved Environments is still Customer PHI, and Ottoclip will protect it as this BAA requires. Recording flows, or setting content to regenerate, outside the Approved Environments is a violation of this BAA by Customer.

6. TERM AND TERMINATION

6.1 Term. This BAA starts on the Effective Date and lasts until the Agreement ends or either party ends this BAA under Section 6.2 or 7.2. Ottoclip's duties under this BAA continue for any Customer PHI it still holds after that, until the information is returned or destroyed under Section 6.3.

6.2 Ending for a violation. If either party learns that the other has violated a material term of this BAA, it will give the other written notice and 30 days to fix the violation. If the violation is not fixed in that time, or cannot be fixed, the party that gave notice may end this BAA and the parts of the Agreement that involve Customer PHI.

6.3 Return or destruction. Within 30 days after this BAA ends, Ottoclip will destroy all Customer PHI it and its Subcontractors hold, including in its database, its cloud storage, and the computers that generate content. If Customer asks before this BAA ends, Ottoclip will first give Customer an export of its content. Customer PHI held in backups will be destroyed as those backups expire, within [backup retention period] days, and stays protected by this BAA until then. If returning or destroying any Customer PHI is not feasible, Ottoclip will tell Customer why, keep that information protected by this BAA, and limit further uses and disclosures to the purposes that make return or destruction not feasible, for as long as Ottoclip holds it. On request, Ottoclip will confirm the destruction in writing.

6.4 Survival. Sections 4.2, 4.3, 4.10, 6.3, and 7, and any other duty that by its nature should last, continue after this BAA ends for as long as Ottoclip holds any Customer PHI.

7. GENERAL TERMS

7.1 Which document wins. For Customer PHI, this BAA controls if it conflicts with the Agreement or with any other terms between the parties. In particular, the content license Customer grants Ottoclip under the Agreement covers Customer PHI only for providing the Services, and Section 6.3 of this BAA replaces any longer retention period the Agreement allows after Customer deletes content or ends its account.

7.2 Changes in the law. The parties will amend this BAA as needed to keep up with changes to the HIPAA Rules. If they cannot agree on an amendment within 60 days after either party asks for one, either party may end this BAA and the parts of the Agreement that involve Customer PHI. This BAA is to be read in the way that lets both parties comply with the HIPAA Rules.

7.3 References. A reference to a section of the HIPAA Rules means that section as in effect or as amended.

7.4 Independent contractor. Ottoclip acts as an independent contractor and not as Customer's agent.

7.5 No third-party rights. Nothing in this BAA gives any right or remedy to anyone other than Customer and Ottoclip.

7.6 Liability. The limits and exclusions of liability in the Agreement apply to this BAA, unless the order form sets a separate limit for violations of this BAA.

7.7 Notices. Notices under this BAA must be in writing and sent by email with a copy by mail or courier to the addresses below. A report under Section 4.2 takes effect when the email is sent.

(a) Ottoclip: CollectiveSoft, Inc., 808 Bauer Dr, San Carlos, CA 94070, legal@ottoclip.com, attention Privacy and Security Officer.

(b) Customer: [name], [mailing address], [email], attention [title].

7.8 Governing law. California law governs this BAA, except where federal law, including the HIPAA Rules, applies. Disputes under this BAA are resolved as the Agreement provides.

7.9 Signing. The parties may sign this BAA in counterparts and by electronic signature.

7.10 Whole agreement. This BAA and the Agreement are the parties' whole agreement about Customer PHI.

7.11 Changes to this BAA. A change to this BAA, including to Exhibit A, needs a written amendment signed by both parties. Ottoclip may update Exhibit B by notice under Section 4.4.

SIGNATURES

CollectiveSoft, Inc. (Ottoclip)		**[Customer legal name]**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

EXHIBIT A

Services and Approved Environments

Services covered. The Ottoclip [Business / Enterprise] plan. This covers recording with the browser extension, cloud generation and scheduled regeneration, hosting of generated content, and help from Ottoclip staff to set up or repair scripts.

Data in the Approved Environments. Customer will use only demo, test, or de-identified data in the Approved Environments. The parties expect Customer PHI to reach Ottoclip only by mistake, for example a real patient record left in a test environment, and any that does is protected by this BAA. Recording or regenerating content in an environment that holds real patient data is not allowed under this Exhibit and needs a written amendment first.

Approved Environments.

Product	**Web address (host)**	**What data it holds**	**Scheduled regeneration allowed**
[Product name]	[demo.example.com]	[Demo patients only]	[Yes / No]

Sharing. Customer will set generated content that shows Protected Health Information to require sign-in. Other generated content may be shared as Customer chooses.

EXHIBIT B

Subcontractors that may receive Customer PHI

Subcontractor	**What it does for Ottoclip**	**Customer PHI it may receive**	**Business associate agreement in place since**
Google LLC (Google Cloud)	Servers, database, file storage, text-to-speech, and Gemini AI models through Vertex AI	All stored content	[date]
Anthropic, PBC	Claude AI models, used through the Ottoclip developer account its business associate agreement covers, that write and check narration and scripts	Page text, screenshots, and scripts	[date]
Cloudflare, Inc.	Network service that carries traffic between browsers and Ottoclip's web app, including uploads from the browser extension	Recordings, scripts, and content while they travel	[date]
[Other, only if used for Customer's content]	[what it does]	[what it receives]	[date]