BUSINESS ASSOCIATE AGREEMENT (BAA)

CareNotes L.L.C. 120 E 56th St, 6th Floor, New York, NY 10022, United States Contact: info@cnotes.ai

Version: 1.0 • **Last updated:** 2026-07-03

> This is the standard CareNotes Business Associate Agreement. It may be executed as a standalone signed document or accepted electronically as part of the CareNotes Terms of Service. **A separate BAA is executed with each subscribing legal entity**, so a group operating multiple practices under separate LLCs can hold one BAA per LLC.

PARTIES

This Business Associate Agreement (this **"Agreement"**) is entered into by and between:

- **Covered Entity** (*"you," "your,"* or *"Covered Entity"*) — the healthcare provider or practice identified in the signature block below; and
- **CareNotes L.L.C.** (*"CareNotes," "we," "us,"* or *"Business Associate"*).

This Agreement is effective as of the date of last signature below or the date you accept the CareNotes Terms of Service, whichever is earlier (the **"Effective Date"**). It governs the handling of Protected Health Information (**"PHI"**) in accordance with the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**), the Health Information Technology for Economic and Clinical Health Act (**"HITECH"**), and their implementing regulations (collectively, the **"HIPAA Rules"**).

1. DEFINITIONS

- **Business Associate:** CareNotes L.L.C., which performs functions or activities involving PHI on behalf of the Covered Entity.
- **Covered Entity:** The healthcare provider or practice using CareNotes that is subject to the HIPAA Rules.

- **Protected Health Information (PHI):** Individually identifiable health information, as defined at 45 CFR § 160.103, that CareNotes creates, receives, maintains, or transmits on behalf of the Covered Entity. In this Agreement, "PHI" includes electronic PHI ("ePHI").
- **Subcontractor:** A person or entity to whom CareNotes delegates a function, activity, or service involving the use or disclosure of PHI (also referred to as a **subprocessor**).
- All other capitalized terms not defined here have the meanings set forth in the HIPAA Rules.

2. PERMITTED USES & DISCLOSURES

CareNotes may use or disclose PHI only:

- To perform the services described in the Terms of Service (e.g., generating and storing clinical notes from clinician-provided transcript text);
- For the proper management and administration of CareNotes, and to carry out its legal responsibilities, provided that any disclosure is required by law or CareNotes obtains reasonable assurances of confidentiality and breach notification from the recipient;
- For data aggregation services relating to the health care operations of the Covered Entity, as permitted by 45 CFR § 164.504(e)(2)(i)(B);
- To de-identify PHI in accordance with 45 CFR § 164.514(a)–(b), after which the de-identified data is no longer PHI; and
- As **Required by Law**.

CareNotes will not use or disclose PHI in any manner that would violate the HIPAA Rules if done by the Covered Entity, except as permitted above. **CareNotes does not sell PHI and does not use PHI, patient audio, transcripts, generated notes, clinician edits, or prompts to train, fine-tune, or improve AI models** (see the Security & HIPAA Overview and Privacy & Security FAQ).

3. SAFEGUARDS

CareNotes shall:

- Implement appropriate administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI, as required by the HIPAA Security Rule (45 CFR §§ 164.308, 164.310, 164.312, and 164.316);
- Encrypt PHI in transit (TLS) and at rest;
- Apply role-based, least-privilege access controls and audit logging to any access to PHI; and
- Comply with the applicable requirements of the HIPAA Security Rule with respect to ePHI.

4. BREACH NOTIFICATION

CareNotes will:

- Report to the Covered Entity any use or disclosure of PHI not permitted by this Agreement of which it becomes aware, including any Security Incident or Breach of Unsecured PHI;
- Notify the Covered Entity of a Breach of Unsecured PHI without unreasonable delay and in no event later than **sixty (60) calendar days** after discovery, per 45 CFR § 164.410; and
- Include in that notification, to the extent available, the identification of affected individuals and the other information required under 45 CFR § 164.410.

Unsuccessful Security Incidents (e.g., routine pings, port scans, and blocked access attempts that do not result in unauthorized access to PHI) are acknowledged as ongoing and are reported only on the Covered Entity's request in aggregate form.

5. SUBCONTRACTORS & SUBPROCESSORS

CareNotes will ensure that any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of CareNotes agrees in writing to restrictions and conditions on the PHI that are at least as protective as those in this Agreement (45 CFR § 164.502(e)(1)(ii) and § 164.308(b)(2)).

CareNotes maintains a current list of PHI subprocessors and the safeguards that apply to each; see the **Subprocessor List**. CareNotes' AI providers process PHI under their own Business Associate Agreements and are contractually prohibited from using submitted data for model training.

6. INDIVIDUAL RIGHTS

CareNotes will assist the Covered Entity in meeting its obligations to individuals by:

- Making PHI available for access as required by 45 CFR § 164.524, within thirty (30) days of the Covered Entity's request;
- Making PHI available for amendment and incorporating amendments as required by 45 CFR § 164.526;
- Making available the information required to provide an accounting of disclosures under 45 CFR § 164.528; and
- Making its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services for purposes of determining compliance with the HIPAA Rules.

7. RETURN OR DESTRUCTION OF PHI

Upon termination of this Agreement or the Covered Entity's use of CareNotes, CareNotes shall, if feasible, return or securely destroy all PHI received from, or created or received on behalf of, the Covered Entity that CareNotes still maintains. Where return or destruction is not feasible (for example, PHI retained in encrypted disaster-recovery backups), CareNotes shall extend the protections of this Agreement to that PHI and limit further uses and disclosures to those purposes that make return or destruction infeasible, until the PHI is destroyed in accordance with the **Data Retention & Deletion Policy**.

8. TERM & TERMINATION

This Agreement is effective as of the Effective Date and remains in effect until all PHI is returned or destroyed, or the protections of Section 7 are extended to any PHI retained. Either party may terminate this Agreement for a material breach that is not cured within thirty (30) days of written notice. If cure is not feasible, the non-breaching party may terminate immediately.

9. NO WARRANTY

Except as expressly stated in this Agreement or required by law, CareNotes provides the platform and services *"as-is"* and makes no warranties, express or implied.

10. GOVERNING LAW

This Agreement is governed by applicable U.S. federal law (including the HIPAA Rules) and the laws of the State of New York, without regard to conflict-of-law principles.

11. INCORPORATION INTO TERMS OF SERVICE

This Agreement is incorporated by reference into the CareNotes Terms of Service. In the event of a conflict between this Agreement and the Terms of Service with respect to PHI, this Agreement controls. If any term is inconsistent with the HIPAA Rules, the parties will interpret it to comply with the HIPAA Rules.

12. CONTACT INFORMATION

Questions about this Agreement or CareNotes' PHI practices: Email: **info@cnotes.ai**

SIGNATURES

Covered Entity

Legal entity name _____

Authorized signatory (print) _____

Title _____

Signature _____

Date _____

Business Associate — CareNotes L.L.C.

Authorized signatory (print) _____

Title _____

Signature _____

Date _____

> **Multiple practices:** To execute a separate BAA for each of your legal entities, complete one copy of this Agreement per LLC. Each executed BAA stands on its own.