

HIPAA BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is entered into on _____ (the “Effective Date”), by and between _____ (“Covered Entity”) and **SureVisit Health, LLC** (“Business Associate”).

1. Purpose and Scope

Covered Entity is a “covered entity” as defined by HIPAA. Business Associate provides a web-based scheduling SaaS, practice analytics, and automated notification services (the “Services”) that may require the creation, receipt, maintenance, or transmission of Protected Health Information (“PHI”). This Agreement ensures that both parties comply with HIPAA, the HITECH Act, and the Omnibus Rule of 2013.

2. Definitions

- **PHI:** Shall have the same meaning as the term “protected health information” in 45 CFR § 160.103.
- **Browser Bridge:** Refers to the proprietary software utility used to sync appointment and patient data from the SureVisit Health platform into the Covered Entity’s EHR.

3. Obligations of SureVisit Health (Business Associate)

3.1 Technical Infrastructure and Safeguards Business Associate maintains a dedicated HIPAA-compliant environment utilizing industry-leading subcontractors for hosting and communications. Security protocols include:

- **Secure Hosting (HIPAAVault):** All data hosting and processing occur on dedicated, audited servers with managed firewalls, intrusion detection (IDS),

and 24/7/365 monitoring with monitored and controlled access to data centers. SureVisit Health maintains detailed logs for all logins and activity to both SureVisit Health administrative website access and client practice accounts.

- **Secure data backup:** All SureVisit Health website data is backed up daily to **iDrive** HIPAA-compliant environment. Data is encrypted both in Transit and at Rest with 256-bit AES and secure, SOC-approved, and monitored data centers in the United States. iDrive maintains audit trails with detailed logs maintained for logins, file modifications, and restores. iDrive maintains strict, controlled access to data centers.
- **Encrypted Email Notifications (Sinch by Mailgun):** All patient-facing emails are transmitted via HIPAA-compliant, encrypted channels utilizing TLS (Transport Layer Security) to protect data in transit.
- **Encrypted SMS Notifications (Telnix):** All text-based reminders and notifications are processed without PHI (not requiring HIPAA). Nonetheless, we follow strict SMS protocols, ensuring a "Minimum Necessary" standard. All messages are encrypted during transmission using a dedicated and verified 10DLS number and SureVisit Health and Telnix enforce 10DLS industry compliance.
- **Data at Rest:** All PHI stored within the SureVisit environment is encrypted using FIPS 140-2 validated encryption modules.
- **Data in Transit:** All connections between the User's browser, the Smart Scheduler, and the Browser Bridge are encrypted via TLS 1.2 or higher.

3.2 Reporting of Violations Business Associate shall notify Covered Entity of any "Breach" of unsecured PHI or any "Security Incident" within **ten (10) business days** of discovery.

3.3 Subcontractors Business Associate shall ensure that all subcontractors (including **HIPAAVault**, **Sinch by Mailgun**, and **iDrive**) that create, receive, maintain, or transmit PHI agree to the same restrictions and conditions that apply to the Business Associate under this Agreement.

4. Permitted Uses and Disclosures

Business Associate is authorized to use and disclose PHI for the following purposes:

- **Automated Notifications:** Utilizing encrypted email to provide appointment confirmations, reminders, and rescheduling links to patients.
- **EHR Integration:** Executing the one-way sync of patient data into the Covered Entity's EHR via the **Browser Bridge** as initiated by the Covered Entity's staff.
- **Practice Analytics:** Providing the Covered Entity with dashboard insights regarding practice performance and staff efficiency using data collected via the Services.
- **Administration:** For the proper management and administration of the Business Associate or to carry out its legal responsibilities.

5. Term and Termination

- **Term:** This Agreement shall be effective as of the Effective Date and shall terminate when the underlying Service Agreement expires.
- **Disposition of PHI:** Upon termination, Business Associate shall, if feasible, return or destroy all PHI received from Covered Entity. If return or destruction is not feasible, Business Associate shall continue to extend the protections of this Agreement to the retained PHI.

-

6. Miscellaneous

- **Amendment:** The Parties agree to take such action as is necessary to amend this Agreement as needed to comply with the requirements of HIPAA.
- **Regulatory References:** A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

Covered Entity: _____

Signature: _____

Title: _____

Date: _____

SureVisit Health, LLC (Business Associate):

Signature: _____

Title: Founder / President

Date: _____