

BUSINESS ASSOCIATE AGREEMENT

If Customer is a Covered Entity or a Business Associate and uses the Subscription Services or Software to transmit, store, or otherwise process Protected Health Information (“PHI”), acceptance of your applicable terms of service (e.g., the applicable standard Terms and Conditions (www.zix.com/terms) (“**Underlying Agreement**”), incorporates the terms of this HIPAA Business Associate Agreement (“BAA”) into the Underlying Agreement. If there is any conflict between a provision in this BAA and a provision in the Underlying Agreement, this BAA will control.

1. Definitions.

Except as otherwise defined in this BAA, capitalized terms shall have the definitions set forth in HIPAA and the Underlying Agreement.

- a. **“Breach Notification Rule”** means the Breach Notification for Unsecured Protected Health Information Final Rule.
- b. **“Business Associate”** shall have the same meaning as “business associate” in 45 CFR § 160.103.
- c. **“Covered Entity”** shall have the same meaning as “covered entity” in 45 CFR § 160.103.
- d. **“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996.
- e. **“Privacy Rule”** means the Standards for Privacy of Individually Identifiable Health Information.
- f. **“Protected Health Information” and PHI** shall have the same meaning as “protected health information” in 45 CFR § 160.103, provided that it is limited to such protected health information that is received, created, maintained, or transmitted by Provider on behalf of Customer.
- g. **“Provider”** means a Zix Corp Group entity that provides the applicable service.
- h. **“Required By Law”** shall have the same meaning as “Required by Law” in 45 CFR § 160.103.
- i. **“Security Rule”** means the Security Standards for the Protection of Electronic Protected Health Information.
- j. **“Zix Corp Group”** means ZixCorp Systems, Inc., including any of its affiliates such as AppRiver, LLC, Greenview Data, Inc., and CM2.COM, Inc. dba Erado.

2. Obligations and Activities of Provider.

To the extent Provider is acting as a Business Associate, Provider shall:

- a. **Use and Disclosure.** Not use or disclose PHI other than as permitted or required by this BAA or as Required By Law.
- b. **Security Rule Safeguards.** Use reasonable and appropriate safeguards and comply, where applicable, with the Security Rule with respect to PHI, to prevent use or disclosure of PHI other than as permitted or required by this BAA or as Required By Law.
- c. **Reporting.** Report to Customer any use or disclosure of PHI not provided for by this BAA of which Provider becomes aware as required by 45 CFR § 164.410, including breaches of unsecured PHI and Security Incidents except for unsuccessful ones. Notification of a Breach will be made without unreasonable delay after discovery and within applicable legal requirements, such as 72-hours under General Data Protection Rule. Provider’s notice to Customer of an unauthorized access, use or disclosure shall contain information sufficient to enable Customer to meet the requirements for notification set forth in 45 CFR § 164.404(d)(1). Notice is hereby deemed given for Security Incidents that are unsuccessful. This includes, without limitation: pings and other broadcast attacks, scans, unsuccessful log-on attempts, and denial of service attacks, so long as no such incident results in unauthorized access, use or disclosure of Customer’s PHI.
- d. **Subcontractors.** In accordance with 45 CFR § 164.502(e)(1)(ii) and 164.308(b)(2), ensure that subcontractors that create, receive, maintain or transmit PHI on behalf of Provider agree to the same restrictions and conditions that apply to Provider with respect to such PHI.
- e. **Access.** Make available to Customer any PHI in a designated record set maintained by Provider as needed to satisfy Customer’s obligations under 45 CFR § 164.524.
- f. **Amendment.** Maintain and make available to Customer for amendment any PHI in a designated record set maintained by Provider, and incorporate any amendments to such PHI, as needed to satisfy Customer’s obligations under 45 CFR § 164.526.
- g. **Accounting of Disclosure.** Make available to Customer the information required to provide an accounting of disclosures as needed to satisfy Customer’s obligations under 45 CFR § 164.528.
- h. **Performance of a Customer’s Obligations.** To the extent that Provider is to carry out Customer’s obligation under the Subpart E of 45 CFR § 164 (Privacy Rule), comply with the requirements of Subpart E that apply to Customer in the performance of such obligation.
- i. **Disclosure to the Secretary.** Make Provider’s internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA rules.

3. Permitted Uses and Disclosures by Provider.

Except as otherwise limited in this BAA, Provider may use and disclose PHI to perform functions, activities or services for, or on behalf of, Customer as described in the Underlying Agreement, which is incorporated by reference; provided that any such use or disclosure would not violate HIPAA if done by Customer, unless expressly permitted by this Section 3.

Except as otherwise limited in this BAA, Provider may use PHI to carry out its legal responsibilities, and the management and administration of Provider, and Provider may disclose PHI for those purposes if the disclosure is (i) Required By Law or (ii) Provider obtains reasonable assurances from the person to whom the PHI is disclosed that the PHI will be held confidentially and be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies Provider of any instances of which it is aware in which the confidentiality of the PHI has been breached.

4. Obligations and Activities of Customer.

- a. **Permissible Requests Only.** Customer shall not request Provider to disclose PHI in any manner that would not be permissible under HIPAA Regulations if done by Customer (e.g. social media).
- b. **Safeguards and Appropriate Use.** Customer is responsible for implementing appropriate privacy and security safeguards to protect PHI in compliance with HIPAA. With respect to Customer Data, once it is sent over the public Internet to or from Customer outside of Provider encryption or other service, Provider does not act as, or have the obligations of, a Business Associate under HIPAA with respect to Customer Data.
- c. **Restrictions.** Customer will notify Provider of any restriction to the use or disclosure of PHI that Customer has promulgated, agreed to, or is required to abide by under HIPAA, to the extent that such restriction may affect Provider's use or disclosure of PHI.

5. Applicability.

This BAA is applicable to Provider services.

6. Term and Termination.

- a. **Term and Expiration.** This BAA will expire when Provider has, after termination of the Underlying Agreement, returned to Customer or destroyed all PHI that Provider received from, or created or received on behalf of, Customer.
- b. **Early Termination.** Each party has the right to terminate this BAA and the Underlying Agreement if it determines either that, the other party has violated a material term of this BAA, following notice and a 30-day cure period.
- c. **Effect of Termination.** At termination of this BAA or the Underlying Agreement, if feasible, return or destroy all PHI that Provider received from, or created or received on behalf of, Customer that Provider still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of this BAA to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

7. Amendment and Interpretation.

The parties shall amend this BAA from time to time as necessary for Customer and Provider to comply with the HIPAA Regulations. Any ambiguity in this BAA will be resolved to permit Customer to comply with the HIPAA Regulations. Except as set forth in this BAA, the parties' respective rights and obligations are defined in and by the Underlying Agreement. Nothing in this BAA is intended to convey any rights, remedies or other benefits on any person or entity other than the parties to this BAA.