Tebra Terms of Service

PLEASE READ THESE TERMS OF SERVICE CAREFULLY BEFORE USING THIS SERVICE. KAREO AND PATIENTPOP HAVE JOINED FORCES AS TEBRA TO UNLOCK BETTER HEALTHCARE WITH AN OPERATING SYSTEM FOR THE CONNECTED PRACTICE OF THE FUTURE. AS PART OF THIS EXCITING TRANSITION, WE ARE UNIFYING OUR TERMS OF SERVICE TO IMPROVE OUR USER EXPERIENCE AND CLEARLY CONVEY YOUR AND OUR RIGHTS AND RESPONSIBILITIES. EFFECTIVE JUNE 1, 2023, THE TEBRA TERMS OF SERVICE SET FORTH BELOW WILL SUPERSEDE AND REPLACE THE CURRENT KAREO TERMS OF SERVICE AND THE PATIENTPOP TERMS OF SERVICE. THESE TERMS OF SERVICE ARE BY AND BETWEEN TEBRA TECHNOLOGIES, INC., INCLUDING ITS SUBSIDIARY, PATIENTPOP, INC. (TEBRA) AND THE INDIVIDUAL(S) OR ENTITY(IES) NAMED ON ONE OR MORE ORDER FORMS OR SUBSCRIPTION AGREEMENTS WITH TEBRA (THE CUSTOMER). BY USING THE SERVICES DESCRIBED BELOW, CLICKING A BOX INDICATING ACCEPTANCE, OR EXECUTING AN ORDER FORM OR SUBSCRIPTION AGREEMENT REFERENCING THESE TERMS OF SERVICE, CUSTOMER IS AGREEING TO BE BOUND BY THESE TERMS OF SERVICE. IF YOU DO NOT AGREE TO THESE TERMS OF SERVICE, DO NOT SUBSCRIBE TO, ACCESS, OR USE THE SERVICE.

1) TEBRA SOFTWARE SERVICES

- These Terms of Service provide the Customer with access and use of Tebra's services, as specified on the applicable order form or subscription agreement between the parties. These Terms of Service, along with the applicable order form or subscription agreement, are referred to herein collectively as the **Customer Agreement.** Customer may purchase services across Tebra's solutions offerings, which are collectively referred to as the **Service**.
- **Policies.** Customer understands that use of the Service is also governed by our Privacy Policy, Pricing Policy, Business Associate Agreement, Support Policy, and Security Notice, as they each may be modified over time.

2) RESPONSIBILITIES

a) Tebra Support Responsibilities

i) Support

Tebra will provide customer support for the Service as further detailed in the Support Policy.

b) Customer Responsibilities

i) Access by Employees and Contractors

- Customer may not make the Service available to anyone other than its employees and contractors and will do so solely to access the Service for the benefit of Customer in compliance with the terms of these Terms of Service.
- Customer is responsible for the compliance with these Terms of Service by its employees and contractors.

ii) Restrictions

Customer may not:

- sell, resell, rent, or lease the Service, or use the Service beyond its internal operations;
- use the Service to store or transmit unsolicited marketing emails or infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights (including without limitation any privacy rights);
- interfere with or disrupt the integrity or performance of the Service;
- attempt to gain unauthorized access to the Service or its related systems or networks;
- modify, copy the Service, or create derivative works based on the Service or any part, feature, function, or user interface;
- except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Service or remove or modify any proprietary marking or restrictive legends in the Service;
- use the Service in violation of any law; or
- access the Service to build a competitive service or offering.

c) Customer Information

i) Customer Information

All data, information, images, documentation, and files entered or uploaded by Customer to the Service remains the property of Customer, as between Tebra and Customer (Customer Information), subject to the other terms of these Terms of Service.

ii) License to Use Customer Information

Customer grants Tebra a non-exclusive, royalty-free, license to modify, store, transmit, and otherwise use the Customer Information for purposes of Tebra performing under these Terms of Service.

iii) Responsibility for Customer Information

Customer is solely responsible for Customer Information including, must use commercially reasonable efforts to prevent unauthorized access to the Service, must notify Tebra promptly of any known unauthorized access, and may use the Service only in accordance with its intended purposes and applicable law.

iv) Accuracy of Customer Information

Customer represents and warrants to Tebra that all Customer Information, and any other material provided under Customer's account, by Customer or on its behalf, is true, correct, and accurate. If Customer learns that any Customer Information provided to Tebra as part of the Service is not true, correct or accurate, Customer must immediately notify Tebra by phone and in writing of this fact, and provide the true, correct and accurate information to Tebra. Tebra relies on Customer representations regarding the truth, accuracy and compliance with laws concerning Customer Information. TEBRA IS NOT LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY CUSTOMER'S FAILURE TO COMPLY WITH THIS PARAGRAPH, IRRESPECTIVE OF ANY ACT OR OMISSION ON THE PART OF TEBRA.

d) 'Tebra Clinical' Service Offering – Additional Terms.

i) Electronic Prescriptions for Controlled Substances

If Customer uses the Services for Electronic Prescriptions for Controlled Substances (**EPCS**), the following applies:

(1) Tokens

a. Each Electronic Prescription account is assigned to a specific provider (**Prescribing Provider**) authorized by Customer.
b. Each Prescribing Provider will be provided with a complimentary Identity-Proof Hard Token (**Hard Token**) and confirmation letter.
c. If the Hard Token is lost, damaged, or becomes inoperable, there will be an additional fee for a new Hard Token or confirmation letter.
d. If Prescribing Provider secures and elects to use a Soft Token (**Soft Token**) provided by a third-party, the Soft Token *must be downloaded and stored on a separate device* from the computer or device on which the Prescribing Provider gains access to the EPCS feature and transmits prescriptions.

The Hard Tokens and Soft Tokens are referred to generally as Tokens.

(2) Customer Responsibilities

Customer and each Prescribing Provider agrees:

a. that each Prescribing Provider retains sole possession of the Hard Token and not to share the login passphrase with any other person;
b. that each Prescribing Provider may not allow any other person to use the Token or enter the login passphrase in order to sign controlled substance prescriptions;
c. that failure to secure the Token, login passphrase, or any biometric information may provide a basis for revocation or suspension of the EPCS account;
d. to notify Tebra within one (1) business day of discovery if:
    i. Customer or a Prescribing Provider is contacted by a pharmacy because one or more controlled substance prescriptions are displaying the incorrect United States Drug Enforcement Administration (**DEA**) number;
    ii. if Customer or a Prescribing Provider discovers that one or more controlled substance prescriptions issued using a Prescribing Provider DEA number were not consistent with the prescriptions actually signed, or were not signed at all; or
    iii. if a Prescribing Provider's Token has been lost or stolen, or the authentication protocol has been compromised in any way;
e. that the Prescribing Provider is responsible for any controlled substance prescriptions written using its two-factor authentication credential;
f. that Prescribing Providers have the same responsibilities when issuing electronic prescriptions for controlled substances as when issuing paper or oral prescriptions;
g. to prescribe controlled substances only for legitimate medical purposes;
h. to review security logs on a daily basis for any security incidents, and to report to the DEA any security incident and provide Tebra with a copy of such report; and
i. to keep all security incident reports on file for a period of two (2) years.

(3) EPCS and Prescription Drug Monitoring Program (PDMP)

Access and use of EPCS with PDMP add-on service by Customer is subject to and governed by the third party terms here: https://drfirst.com/epcs-pdmp-terms-of-use/.

(4) Electronic Prescriptions Excluding Prescriptions for Controlled Substances (Non-EPCS Electronic Prescriptions)

If Customer uses the Service for Non-EPCS Electronic Prescriptions, the Customer and each Prescribing Provider agrees:

a. to only prescribe on their own behalf and not give away password or credentials to another person to prescribe for them; and
b. to take the same responsibility as Customer would take when transmuting paper or phone prescriptions.

(5) Meaningful Use

Customer and providers intending to attest for Meaningful Use agree to follow the processes and procedures recommended in Tebra's Meaningful Use training such that Tebra's tracking and reports function appropriately.

(6) Tebra Billing for Mac

Access and use of Tebra Billing by Customer by means of a Mac device is subject to and governed by the third party terms here: https://www.parallels.com/about/legal/eula/.

e) 'Provider Website' 'Practice Growth and 'Engagement Software' Offerings – Additional Terms.

In connection with its Practice Growth and other patient engagement offerings, Tebra may design and develop a cloud-based provider website (Provider Website), and provide cloud-based tools and services (for example, online booking tool, call tracking, reputation management, profile syndication and management, analytics dashboard, and general online local marketing services) (collectively, the Practice Growth and Engagement Software).

The Service includes any required, usual, appropriate, or acceptable methods to perform activities related to the Service, for example:

- conducting analytics and other product improvement activities;
- carrying out the Service or the business of which the Service is a part;
- carrying out any benefits, rights, and obligations related to the Service;
- maintaining records relating to the Service; and
- complying with any legal or self-regulatory obligations related to the Service.

i) Provider Website

1. Provider Website will integrate elements of the Practice Growth Software, including but not limited to the Tebra online booking tool.
2. Customer may, but is not required to, submit Content for inclusion on such Provider Website.

ii) Content Rights

1. Customer may upload or submit content, files, and information to the Service for a Provider Website or other use with the Practice Growth and Engagement Software

(**Content**). Customer retains copyright and any other proprietary rights that Customer may hold in the Content that Customer provides to Tebra; for clarity, all other elements of the Provider Website, Practice Growth and Engagement Software and Content provided by Tebra, apart from any Content provided by Customer, are owned solely by Tebra, and will not be retained by Customer upon suspension, expiration or termination of this agreement.

2. Customer is solely responsible for any Content that Customer provides or any custom tracking technology used on a Provider Website, and for the consequences of posting or publishing such Content or tracking technology.
3. Customer hereby grants Tebra a non-exclusive irrevocable, perpetual, royalty-free license to display, store, distribute, share, modify, and otherwise use such Content for purposes providing the Service under this agreement (including, without limitation, a license to syndicate the Content to third party publisher sites as required to provide Customer the applicable Service (e.g., Tebra Engage)).

iii) Content Warranties

Customer represents and warrants to Tebra that:

1. Any Content submitted to the Service does not violate any copyright, trade secret, privacy or other third party right;
2. It will not submit any Content that is untrue, defamatory, harmful to any person, or violates HIPAA Privacy Rules, state or federal laws on patient privacy; and
3. All patient testimonials submitted by Customer are accurate, have the patient's consent, and comply with ethical guidelines of professional medical associations as well as state and local medical and private practice boards and governing bodies.

iv) Practice Growth and Engagement Software

1. Where applicable, Tebra will make the dashboard element of the Practice Growth Platform (Dashboard) available to Customer in accordance with these Terms of Service and any other Tebra rules and policies then in effect.
2. The Dashboard allows Customer to set up an account and password to access the Dashboard and set up users (Users).

v) Domain Name Upon Termination

Customer will have the following rights to the Provider Website domain name upon termination or expiration of the Customer Agreement:

1. If the domain name was purchased and registered by Tebra, then Tebra will take reasonable measures to assign its rights in the domain name to Customer; or
2. If rights to the domain name were provided by Customer, then Customer will retain such rights to the domain name.

vi) Reviews & Opinions

1. Tebra does not endorse, validate as accurate, or necessarily agree with any of the reviews, links, and user-generated content from users or Customers on the Service.
2. Tebra reserves the right to refuse to publish any patient review provided by Customer.
3. The Service may attempt to send automated or human-based alerts when reviews are provided on third party websites, but Tebra does not guarantee the accuracy, completeness, or timeliness of such alerts.

vii) Advertisements

1. Tebra reserves the right to place advertisements or messages from third parties on free claimed listings web pages as well as free versions of the Service.
2. Such advertisements or messages from third parties may be visible to users as well as Customer.

f) 'Tebra Telehealth' Service Offering – Additional Terms.

i) Telehealth Medical Services

1. Tebra Telehealth is designed to facilitate Customer's delivery of Telehealth Medical Services.
2. Telehealth Medical Services means the delivery of medical care by Customer to a patient physically located at another site through the use of advanced telecommunications technology that allows providers to remotely see and hear the patient in real time.

ii) Customer's Responsibilities

Customer is solely responsible for:

1. the provision of Telehealth Medical Services and all other professional medical services and aspects relating to Customer's practice of medicine (for the avoidance of doubt, Telehealth Medical Services are performed by Customer for appropriate visits as determined in Customer's, or its provider's, as applicable, sole professional judgment);
2. documenting the Telehealth Medical Services in Customer's clinical records;
3. billing and collecting for Telehealth Medical Services;
4. providing notice to and/or obtaining consent from any third parties relating to the provision of Telehealth Medical Services through Tebra Telehealth;
5. ensuring Tebra Telehealth is used in accordance with applicable instructions, training materials and other online material that may be made available by Tebra from time to time;

6. obtaining and maintaining both the functionality and security of all information technology software solutions and related services necessary to connect to, access or otherwise use Tebra Telehealth; and
7. complying with applicable laws and standards imposed by government health care programs and other payors, licensing agencies and applicable accreditation bodies, including, without limitation, with respect to the provision of Telehealth Medical Services.

g) 'Tebra Payment Processing Service' Offering – Additional Terms

If Customer contracts for Payment Processing Services, the Payment Processing Services will be governed by Tebra Payment Processing Terms. If there is a conflict between the Payment Processing Terms and any other terms in the Customer Agreement, the Payment Processing Terms will control for purposes of the Payment Processing Services.

3) PAYMENT TERMS

a) Payment

i. Customer must pay all fees as specified on the order and related services as incurred as specified on the **Pricing Policy** page.
ii. Unless otherwise stated, invoiced charges are due upon receipt.
iii. Customer is responsible for providing complete and accurate billing and contact information to Tebra and notifying Tebra of any changes to such information.

b) Credit Card and ACH

i. Customer must pay all fees (in US dollars) with a credit card or via ACH upon receipt of an invoice from Tebra.
ii. If the credit card or ACH is not valid or the payment is not otherwise made, Customer must pay the amount owed upon receipt of an invoice.
iii. Customer hereby authorizes Tebra to charge such credit card or withdraw from Customer's bank account via ACH for all purchased Services and related services, and any renewals.
iv. **Individual large credit card payments are subject to a processing fee as detailed in the Pricing Policy.**

c) Taxes

i. Except for certain state sales taxes as noted on Customer invoices, Tebra's fees do not include any taxes, levies, or other similar governmental assessments (**Taxes**).
ii. Except as otherwise stated herein, Customer is responsible for the payment of all Taxes associated with its purchases under the Customer Agreement.

iii. Tebra is solely responsible for taxes assessable against Tebra based on its income, property, and employees.

d) Suspension of Service for Non- Payment

i. Tebra may suspend or terminate Customer's access to the Service, or both, if Customer has not paid amounts owed to Tebra when due.
ii. In advance of any suspension or termination, Tebra will make commercially reasonable efforts to send a minimum of five (5) days' advance electronic notice of payment default to the email address in Customer's account within the Service.
iii. **Tebra reserves the right to assess a reactivation fee, as detailed in the Tebra Pricing Policy to Customers whose accounts are suspended based on late payments received more than fifteen (15) days following the payment due date.**

e) Fee Changes

i. For Customers with month-to-month agreements, all fees may be changed with sixty (60) days' notice to Customer.
ii. For all Customers, Tebra reserves the right to increase its prices by no greater than 4.9% at any one time, no more frequently than once per twelve- (12-) month period, upon thirty (30) days' notice to the Customer.
iii. For all Customers, Tebra may increase fees to cover the cost of postage rate increases as well as regulatory, compliance, and other cost increases imposed by changes to applicable federal and state rules. Tebra will automatically apply the rate increase to all services impacted by the change with thirty (30) days' notice to the Customer.

f) Timing of Payment

Fees, as identified on the order form or subscription agreement, are due as indicated. Tebra will have the right to charge the Customer's card or debit from Customer's account through ACH for fees in accordance with the agreement. By providing Tebra with payment information, Customer agrees that Tebra is authorized, to the extent permitted by applicable law, to immediately charge such payment method for all fees and charges due and payable to Tebra hereunder and that, except as required by applicable law, no additional notice or consent is required. Customer agrees to immediately notify Tebra of any change in the payment information used for payment hereunder. Customer understands and acknowledges that all amounts owed must be paid in advance and that if timely payment is not received, in addition to being in breach of Customer's contractual obligations, the Service may be paused or terminated. Any amounts not paid by the Customer when due may bear interest at the rate of 1.5% per month (or the highest rate permitted by law). Customer agrees to pay all costs of collection, including attorney's fees and costs and all other legal and collection

expenses incurred by Tebra in connection with its enforcement of its rights under the agreement.

4) REPRESENTATIONS AND WARRANTIES; DISCLAIMERS

a) Availability

Tebra will make commercially reasonable efforts to maintain uptime of 99% excluding any scheduled downtime, force majeure issues and third party services (see Support Policy for additional details).

b) Mutual Representations and Warranties

Each party represents and warrants to the other that:

i. the Customer Agreement has been duly entered into and constitutes a valid and binding agreement enforceable against such party in accordance with its terms;
ii. no authorization or approval from any third party is required in connection with such party's entering into or performance of the Customer Agreement; and
iii. the entering into and performance of the Customer Agreement does not and will not violate the laws of any jurisdiction or the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.

c) DISCLAIMERS

- **TEBRA DISCLAIMS ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE, OR WITHOUT DELAY, AND THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.**
- **WHILE TEBRA TAKES REASONABLE PHYSICAL, TECHNICAL, AND ADMINISTRATIVE MEASURES TO SECURE THE SERVICE, TEBRA DOES NOT GUARANTEE THAT THE SERVICE CANNOT BE COMPROMISED. TEBRA DISCLAIMS ANY WARRANTY REGARDING ANY PERCENTAGE OF COLLECTION OF CLAIMS FOR CUSTOMER.**
- FROM TIME TO TIME, CUSTOMER MAY REQUEST THE ADDITION OF CERTAIN CODE AND/OR FUNCTIONALITIES TO BE ADDED TO CUSTOMER'S WEBSITE OR OTHER PLATFORM. TEBRA SHALL NOT BE RESPONSIBLE FOR ENSURING THAT THE REQUESTED CODE AND/OR FUNCTIONALITIES COMPLY(IES) WITH ANY AND ALL APPLICABLE LAWS AND REGULATIONS PERTAINING TO CUSTOMER'S BUSINESS. CUSTOMER HEREBY ACKNOWLEDGES AND AGREES THAT CUSTOMER ALONE SHALL BE RESPONSIBLE FOR ENSURING THAT CUSTOMER'S WEBSITE AND SERVICE OFFERINGS, EVEN IF SUPPORTED BY TEBRA, COMPLY WITH APPLICABLE LAWS AND REGULATIONS.

5) COMPLIANCE

a) No Medical Advice Provided by Tebra

i. Tebra does not provide medical advice, provide medical or diagnostic services, or prescribe medication.
ii. Use of the Service is not a substitute for the professional judgment of health care providers in diagnosing and treating patients.
iii. Customer agrees that it is solely responsible for verifying the accuracy of patient information (*including, without limitation, obtaining all applicable patients' medical and medication history and allergies), obtaining patient's consent to use the Service (including, without limitation, the Patient Portal*), and for all of its decisions or actions with respect to the medical care, treatment, and well-being of its patients, including without limitation, all of Customer's acts or omissions.
iv. Any use or reliance by Customer upon the Service will not diminish that responsibility.
v. Customer assumes all risks associated with Customer's clinical use of the Service for the treatment of patients.
vi. NEITHER TEBRA NOR ITS LICENSORS ASSUME ANY LIABILITY OR RESPONSIBILITY FOR DAMAGE OR INJURY (INCLUDING DEATH) TO CUSTOMER, A PATIENT, OTHER PERSONS, OR TANGIBLE PROPERTY ARISING FROM ANY USE OF THE SERVICE.

b) Customer's Compliance with Medical Retention Laws and Patient Records Access

i. Customer is responsible for understanding and complying with all state and federal laws related to retention of medical records, patient access to information, and patient authorization to release data.
ii. Customer must obtain any necessary patient consent prior to using the Service (*including, without limitation, the Patient Portal*) and will apply settings to exclude information from availability in the Patient Portal as necessary to comply with state or federal law.

c) HIPAA

i. As part of the Service, Tebra may perform or assist in performing a function or activity on Customer's behalf that involves the use and disclosure of Protected Health Information (as defined in 45 C.F.R. 164.501; **PHI**).
ii. The parties may use or disclose such PHI as required by the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**), the Standards for Privacy of Individually Identifiable Health Information (**Privacy Rule**) and the Standards for Security of Electronic Protected Health Information (**Security Rule**) promulgated thereunder, and the Health Information

Technology for Economic and Clinical Health Act (Division A, Title XIII and Division B, Title IV, of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5) (**HITECH Act**).

iii. Capitalized terms used but not otherwise defined have the same meaning given to such terms in HIPAA, the HITECH Act, or any implementing regulations promulgated thereunder, including but not limited to the Privacy Rule and the Security Rule.

iv. In connection with and by agreeing to the Customer Agreement, you and Tebra agree to be bound by the terms of a Business Associate Agreement which is incorporated herein by reference. You (the "**Covered Entity**," as referred to in the Business Associate Agreement) hereby agree that you have read and agree to be bound by the terms of the Business Associate Agreement.

d) CCPA

i. **Definitions.**

1. **CCPA** means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199.95), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 7000 to 7102), and any related regulations or guidance provided by the California Attorney General. For the purposes of this Section, terms defined in the CCPA, including personal information and business purposes, carry the same meaning.
2. For purposes of this Section, "**Customer Personal Information**" means any "personal information" contained within the data that Tebra "processes" (as defined in the CCPA) in connection with performing the Service.

ii. This Section applies solely to the extent that:

- Tebra's provision of the Service is not exempt from the CCPA under California Civil Code sections 1798.145(c)(1)(A) and (c)(1)(B) pertaining to medical information, PHI, providers of health care, and covered entities;
- Customer is a "business" within the meaning of the CCPA; and
- Tebra is processing the personal information of California residents.

iii. Tebra is a service provider. Tebra will not collect, retain, use, disclose or otherwise process Customer Personal Information for any purpose other than for performing the Service, or as otherwise permitted by the CCPA.

iv. Tebra will limit Customer Personal Information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to provide the Service or to achieve another compatible operational purpose.

v. Tebra will not collect, use, retain, disclose, sell, or otherwise make Customer Personal Information available for Tebra's own commercial purposes or in a way that does not comply with the CCPA. Tebra may, however, create and derive from its provision of the Service anonymized and/or aggregated data that does not identify Customer or any consumer or household, and use, publicize, or share with third parties such data to improve Tebra's products and services and for Tebra's other lawful business purposes.

vi. Notwithstanding the foregoing, with Customer's consent, Tebra may share Customer contact information with certain partners we may work with.

vii. Tebra must promptly comply with any Customer request or instruction requiring Tebra to provide, amend, transfer, or delete Customer Personal Information, or to stop, mitigate, or remedy any unauthorized processing unless otherwise permitted by the CCPA.

viii. Notwithstanding anything in the agreement entered, Customer and Tebra acknowledge and agree that Tebra's access to Customer Personal Information is not part of the consideration exchanged by the parties in respect of the Agreement.

ix. Tebra certifies that it understands its obligations under this Section and must comply with them.

x. If a law requires Tebra to disclose Customer Personal Information for a purpose unrelated to the Service, Tebra must first inform Customer of the legal requirement and give Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

xi. Tebra may use a subcontractor to provide or support the provision of the Service. Any subcontractor used must qualify as a service provider under the CCPA and Tebra will not make any disclosures to the subcontractor that the CCPA would treat as a sale.

xii. Customer is solely responsible for:

- identifying whether the CCPA applies to Customer;
- providing any notices of your privacy practices that may be required by CCPA; and
- identifying and responding to verifiable consumer requests to exercise CCPA rights to access, delete, or opt out of the sale of personal information (**CCPA Requests**), including for verifying the identity of consumers submitting CCPA Requests and for evaluating the scope and legality of CCPA Requests.

xiii. Tebra will provide reasonable assistance to Customer in responding to such CCPA Requests, which may include assistance by way of providing self-service functionality. Tebra will treat any CCPA Requests that Customer submits to Tebra as presumptively valid under the CCPA. With respect to CCPA Requests for which Customer requires Tebra to provide assistance, Customer must:

- notify Tebra within five (5) days of its receipt of the CCPA Request by emailing privacy@tebra.com; and
- provide Tebra with the consumer's email address or such other information that would permit Tebra to honor the request.

Customer is solely responsible and liable for responding to the individual's CCPA Request, including without limitation the content and timing of the response, in compliance with the CCPA.

xiv. In response to a verifiable CCPA Request for access to Customer Personal Information that Customer submits to Tebra, within ten (10) business days of Tebra's receipt of such

request from Customer, Tebra will provide Customer with a file that contains the Customer Personal Information that Tebra maintains about the individual via a secure method of transfer. Tebra may withhold from such file any Customer Personal Information that the CCPA does not require to be provided in response to a CCPA Request.

xv. In response to a verifiable CCPA Request for the deletion of Customer Personal Information that Customer submits to Tebra, except as otherwise required by applicable law or permitted by the CCPA, within ten (10) business days of Tebra's receipt of such request from Customer, Tebra will delete the Customer Personal Information, to the extent Tebra maintains such Customer Personal Information about the individual.

xvi. Tebra may delete such Customer Personal Information by anonymizing and/or aggregating the information such that the information does not identify, and is not reasonably capable of identifying, the individual.

xvii. Customer may not direct or otherwise cause Tebra to share any Customer Personal Information with any third party in a manner that may constitute a "sale" as such term is defined in the CCPA.

e) TCPA

i. This Section concerns compliance with the Telephone Consumer Protection Act of 1991, located at 47 U.S.C. §§ 227 et seq., including the implementing regulations therefor located at 47 C.F.R. 64.1200 et seq. (**TCPA**) and the Telemarketing Sales Rule authorized by the Telemarketing and Consumer Fraud and Abuse Prevention Act, located at 15 U.S.C. §§ 6101-6108 (**TSR**) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, located at 15 U.S.C §§ 7701-7713 (**CAN SPAM Act**).

ii. As between Customer and Tebra, Customer must comply and be solely responsible for complying with all laws governing any messages sent or received in connection with its access or use the Service, *including without limitation, the TCPA, TSR, and CAN SPAM Act.*

iii. Customer is responsible for, without limitation, obtaining any legally required consents from all third parties (including its patients or customers) to send and receive any text message and/or emails using the Service and honoring any requests revoking such consent or otherwise "opting-out" of receiving any such messages and/or emails.

iv. Customer is solely liable for, and must indemnify, defend and hold harmless Tebra from and against any and all damages, liabilities, judgments, fees, fines, costs and expenses (including reasonable attorneys' fees) incurred by Tebra arising from any claims, demands or legal actions made against Tebra resulting from Customer's failure to comply with this Section.

f) Anti-Discrimination Policy

i. At Tebra, we strive to create an environment where people are equally valued and where we and our Customers work together to do our part to help end discrimination.
ii. As a result, Tebra has adopted an anti-discrimination policy that includes our Customers.
iii. Tebra will not tolerate Customers who engage in extreme examples of blatant discrimination or verbal aggression in their interactions with Tebra employees or publicly on social channels.
iv. This includes discrimination against or verbal aggression towards any race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status of any person.
v. Customer agrees and understands that violation of this policy by Customer qualifies as a Material Breach of the Customer Agreement pursuant to **Section 8 (TERM, TERMINATION, AND RETURN OF DATA)**.

g) Definition of Confidential Information

i. Confidential Information means all non-public information disclosed by a party **(Discloser)** to the other party **(Recipient)**, whether orally, visually or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure (**Confidential Information**).
ii. Tebra's Confidential Information includes, without limitation, the non-public portions of the Service and Customer's Confidential Information includes, without limitation, Customer Information.

h) Protection of Confidential Information

i. Recipient must use the same degree of care that it uses to protect the confidentiality of its own confidential information (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Discloser for any purpose outside the scope of the Customer Agreement.
ii. Recipient must make commercially reasonable efforts to limit access to Confidential Information of Discloser to those of its employees, contractors, and clients (as the case may be) who need such access for purposes consistent with the Customer Agreement and who have signed confidentiality agreements with Recipient no less restrictive than the confidentiality terms of the Customer Agreement.
iii. Recipient may disclose Confidential Information (1) to the extent required by law or legal process; (2) to its legal or financial advisors, provided that such advisors are bound by a duty of confidentiality that includes use and disclosure restrictions; and (3) as required under applicable securities regulations.

iv. Each party may disclose the terms and conditions of the Customer Agreement on a confidential basis to current and prospective investors, acquirers, lenders, and their respective legal and financial advisors in connection with due diligence activities.

i) Exclusions

Confidential Information excludes information that (1) is or becomes generally known to the public without breach of any obligation owed to Discloser; (2) was known to the Recipient prior to its disclosure by the Discloser without breach of any obligation owed to the Discloser; (3) is received from a third party without breach of any obligation owed to Discloser; or (4) was independently developed by the Recipient without use or access to the Confidential Information.

6) PROPRIETARY RIGHTS

a) Reservation of Rights by Tebra

i. The software, workflow processes, user interface, designs, know-how, and other technologies provided by Tebra as part of the Service, and all updates and enhancements, are the proprietary property of Tebra and its licensors, and all right, title, and interest in and to such items, including all associated intellectual property rights, remain only with Tebra.
ii. Tebra reserves all rights unless expressly granted in the Customer Agreement.

b) AMA Content

Any content of the American Medical Association (**AMA**) is subject to the terms in the **AMA End User License Agreement.**

c) Aggregation Services and De-identified Data

i. Tebra may use PHI to provide Customer with data aggregation services (as that term is defined by HIPAA) and to create de-identified data in accordance with 45 CFR 164.514(a)-(c).
ii. Tebra solely owns all right, title, and interest, in any de-identified data it creates from PHI.
iii. Tebra and its affiliates may use and disclose, during and after the Customer Agreement, all aggregate, anonymized information and de-identified data for purposes of enhancing the Service, technical support and other business purposes, all in compliance with the HIPAA Privacy Standards, including without limitation the limited data set and de-identification of information regulations.

7) LIMITS ON LIABILITY

a) NO INDIRECT DAMAGE

TEBRA WILL NOT BE LIABLE TO CUSTOMER FOR ANY LOST PROFITS, COST OF COVER, LOSS OF DATA, INTERRUPTION OF BUSINESS OR ANY INCIDENTAL, SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, EVEN IF CUSTOMER IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE.

b) LIMIT

i. TEBRA'S TOTAL LIABILITY FOR ALL DAMAGES ARISING UNDER OR RELATED TO THE CUSTOMER AGREEMENT (IN CONTRACT, TORT, OR OTHERWISE) WILL NOT EXCEED THE ACTUAL AMOUNT PAID BY CUSTOMER WITHIN THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE EVENT WHICH GAVE RISE TO THE CLAIM.
ii. THIS LIMITATION OF LIABILITY IS INTENDED TO APPLY WITHOUT REGARD TO WHETHER OTHER PROVISIONS OF THIS AGREEMENT HAVE BEEN BREACHED OR HAVE PROVEN INEFFECTIVE OR IF A REMEDY FAILS OF ITS ESSENTIAL PURPOSE.
iii. ANY CLAIM BY CUSTOMER AGAINST TEBRA MUST BE BROUGHT WITHIN SIX (6) MONTHS OF THE EVENT WHICH GAVE RISE TO THE CLAIM, AND IF IT IS NOT BROUGHT WITHIN SUCH TIME PERIOD THEN SUCH CLAIM IS EXPRESSLY WAIVED BY CUSTOMER.

8) TERM, TERMINATION, AND RETURN OF DATA

a) Term

i. The applicable Services will continue for the duration specified in the applicable Customer Agreement (**Initial Term**)**.** Following the end date of the Initial Term, the Customer Agreement will be automatically extended for additional consecutive terms of equal duration to the Initial Term (**Renewal Term**) unless either party provides notice of non-renewal in accordance with the Section entitled "Notice of Non-Renewal" below. The Initial Term and any subsequent Renewal Term(s) may be collectively referred to as the "**Term**".
ii. These Terms of Service continue in effect until all order forms and/or subscription agreements and all Services are terminated.

b) Notice of Non-Renewal

To prevent renewal of a Customer Agreement, either party must give written notice of non-renewal and this written notice must be received no more than ninety (90) days but no less than sixty (60) days in advance of the end of the Customer Agreement then in effect. If Customer decides not to renew, Customer must send the notice of non-renewal by contacting

the assigned Account Manager directly or via the communications methods in Tebra's Support Policy. Any notice received with less than sixty (60) days' notice will result in auto-renewal of the Customer Agreement for an additional Renewal Term.

c) Downgrades

Customers with Billing, Clinical, Engage, and/or Telehealth modules must provide notice in writing at least thirty (30) days prior to removing a license or canceling a module. Notice should be made to the assigned Account Manager directly or via the communications methods in Tebra's Support Policy.

d) Termination for Material Breach

i. Either party may terminate the Customer Agreement if the other party material breaches any term of the Customer Agreement and does not cure the breach within thirty (30) days of receipt of written or electronic notice of breach.
ii. Additional terms are in the Term, Termination and Return of Data Policy FAQ page.

e) No Early Termination; No Refunds

Absent termination pursuant to the Sections entitled "Notice of Non-Renewal" and "Termination for Material Breach", Customer cannot cancel the Customer Agreement during the Term in effect. Tebra does not provide refunds if Customer decides to stop using the Service before the end of the Term.

f) Return of Data

i. As Customer has access to the Customer Information during the term of an order, Tebra has no obligation to provide Customer Information to Customer upon termination of the Customer Agreement.
ii. Notwithstanding the foregoing, Tebra retains Customer Information for sixty (60) days from such termination and Tebra may provide Customer access to such information upon Customer's request.
iii. Additional information is located at Term, Termination and Return of Data Policy FAQ page.
iv. If Customer's account is suspended for any reason, Tebra will provide *offline access* to Customer Information via the communications methods detailed in the Support Policy.

g) Customer Actions upon Termination

i. Upon termination, Customer must pay any unpaid fees and destroy all Tebra property in Customer's possession.
ii. Customer, upon Tebra's request, will confirm in writing or electronically that it has complied with this requirement.

h) Suspension or Termination of Service for Violation of Law or the Agreement

i. Tebra may immediately suspend or terminate the Service and remove applicable Customer Information if it in good faith believes that, as part of using the Service, Customer may have violated any applicable law or any term of the Customer Agreement.
ii. Tebra may use reasonable efforts to try to contact Customer in advance, but it is not required to do so.

9) INDEMNITY

a) Customer Indemnity

To the maximum extent allowed by law, Customer must indemnify, defend (at Tebra's option), and hold harmless Tebra, including its officers, directors, employees, agents, successors, and assigns against all third-party claims (including, without limitation, by governmental agencies), demands, damages, costs, penalties, fines, and expenses (including reasonable attorneys' fees and costs) arising out of or related to:

i. the use of the Service by Customer;
ii. Customer's breach of any term in the Customer Agreement;
iii. Customer Information;
iv. any unauthorized use, access, or distribution of the Service by Customer; or
v. violation of any individual's privacy rights related to information submitted under Customer's account, or fraudulent, invalid, duplicate, incomplete, unauthorized, or misleading information submitted under Customer's account or by Customer.

b) Tebra Indemnity

Tebra shall indemnify, defend, and hold harmless Customer from and against any and all losses incurred by Customer resulting from any action by a third party (other than an a person or entity that directly or indirectly controls, is controlled by, or is under common control with Customer) against Customer alleging use of the Service in accordance with this Customer Agreement infringes or misappropriates such third party's US Intellectual Property Rights.

The foregoing obligation does not apply to the extent that the alleged infringement arises from:

i. Customer Information or Customer provided Content;
ii. access to or use of the Service in combination with any hardware, system, software, network, or other materials or service not provided by Tebra or specified for Customer's use, unless otherwise expressly permitted by Tebra in writing;

iii. modification of the Service other than:
    1. by or on behalf of Tebra; or
    2. with Tebra's written approval in accordance with Tebra's written specification;
iv. failure to timely implement any modifications, upgrades, replacements, or enhancements made available to Customer by or on behalf of Tebra.

10) DISPUTE RESOLUTION

a) Governing Law

i. The Customer Agreement and any Dispute (as defined below) will be governed exclusively by the laws of the State of California, without regard to its conflicts of laws principles. The Federal District Court for the Central District of California or Orange County Superior court will be the exclusive venue for any resolution of any Dispute. The parties hereby submit to and consent irrevocably to the jurisdiction of such courts for these purposes.
ii. ***The parties hereby irrevocably waive any and all right to trial by jury in any legal proceeding arising out of any Dispute.***

b) General Mediation Process

i. The parties shall submit any and all disputes, claims, or controversies arising out of or relating to the Customer Agreement including any conduct related to or arising out of the Customer Agreement following termination hereof (each a "**Dispute**") as follows:
    1. the parties will submit the dispute to non-binding mediation in Orange County under the mediation rules of the American Arbitration Association (**AAA**); and
    2. if no settlement is reached within sixty (60) days of the start of mediation, either party may seek legal redress in a forum of competent jurisdiction.
ii. Either party may commence mediation by providing to AAA and the other party a written request for mediation, which must set forth the subject of the Dispute, the relief requested, and the factual and legal bases for such relief. The parties shall cooperate with AAA and with one another in selecting a mediator from the AAA panel of neutrals and in scheduling the mediation proceedings. The parties shall participate in the mediation in good faith and equally share the costs of the mediation.
iii. If the Dispute is not resolved through mediation, the party seeking relief may pursue all remedies available at law, subject to the terms of this Agreement.
iv. Notwithstanding this Section, either party may (1) terminate this Agreement according to its terms, or (2) seek injunctive or equitable relief.

c) PROHIBITION OF CLASS AND REPRESENTATIVE ACTIONS

i. EACH PARTY MAY BRING CLAIMS AGAINST THE OTHER ONLY ON AN INDIVIDUAL PARTY BASIS, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE ACTION OR PROCEEDING.
ii. THE MEDIATOR MAY NOT CONSOLIDATE OR JOIN MORE THAN ONE PARTY'S CLAIMS, AND MAY NOT OTHERWISE PRESIDE OVER ANY FORM OF A CONSOLIDATED, CLASS OR REPRESENTATIVE PROCEEDING.

11) OTHER TERMS

a) Consent to Electronic Notice, Communications and Transactions

i. By using the Service, Customer agrees to conduct business electronically and acknowledges that Customer has read the Consumer Disclosure Regarding Electronic Business Transactions, Receiving Electronic Notices and Disclosures, and Signing Documents Electronically, located at https://www.tebra.com/consumer-disclosure/.
ii. For purposes of messages and notices about the Service (including, without limitation, collections and payments issues), Tebra may send email notices to the email address associated with Customer's account or provide in service notifications.
iii. For certain notices (e.g., notices regarding termination or material breaches), Tebra may send notices to the postal address provided by Customer.
iv. Customer is solely responsible for keeping an updated email address within its account for notice purposes.
v. TEBRA HAS NO LIABILITY ASSOCIATED WITH CUSTOMER'S FAILURE TO MAINTAIN ACCURATE CONTACT INFORMATION WITHIN THE SERVICE OR ITS FAILURE TO REVIEW ANY EMAILS OR IN-SERVICE NOTICES.
vi. Customer has the ability to enter into agreements, authorizations, consents, and applications; make referrals; order lab tests; prescribe medications; or engage in other transactions electronically.
vii. ELECTRONIC SUBMISSIONS THROUGH THE SERVICE IN CONNECTION WITH SUCH ACTIVITIES CONSTITUTE CUSTOMER'S CONSENT TO BE BOUND BY SUCH AGREEMENTS AND TRANSACTIONS AND APPLIES TO ALL RECORDS RELATING TO SUCH TRANSACTIONS.
viii. Customer represents and warrants that it has the authority to take such actions.
ix. Customer agrees that by registering for the Service (including without limitation, any request forms or use of communications features), constitutes a request for Tebra to send email, fax, phone call, or SMS communications related to the Service, (including, but not limited to, upcoming appointments, special offers, billing, and upcoming events).
x. Tebra is not responsible for any text messaging or data transmission fees.

xi. If Customer provides a cellular phone number and agrees to receive communications from Tebra, Customer specifically authorizes Tebra to send text messages or calls to such number.
xii. Customer represents and warrants it has the authority to grant such authorization.
xiii. Customer is not required to consent to receive text messages or calls as a condition of using the Service and may opt out of such messages through the Services.

b) Entire Agreement

i. The Customer Agreement constitutes the entire agreement between the parties and supersedes all prior or contemporaneous negotiations or agreements, whether oral or written, related to this subject matter.
ii. Customer is not relying on any representation concerning this subject matter, oral or written, not included in the Customer Agreement.
iii. No representation, promise, or inducement not included in the Customer Agreement is binding.
iv. No modification or waiver of any term of the Customer Agreement is effective unless signed by both parties.
v. Notwithstanding the foregoing, Tebra may modify or replace the Customer Agreement as detailed in the paragraph entitled “Changes”, below.
vi. The Convention on Contracts for the International Sale of Goods does not apply.
vii. If there is a conflict between the Terms of Service and the order form or subscription agreement, the order form or subscription agreement prevails.

c) Changes

Notwithstanding anything to the contrary herein, these Terms of Service are subject to change by Tebra on a going-forward basis in its sole discretion at any time. When changes are made to these Terms of Service, Tebra will make a new copy of the modified Terms available on the Services and will also update the “Last Updated” date at the bottom of the Terms of Service. Any changes to the Terms of Service will be effective immediately for new Customers and will be effective for continuing Customers upon the earlier of: (i) thirty (30) days after posting notice of such changes on the Services for existing Customers; (ii) thirty (30) days after dispatch of an e-mail notice of such changes to you; or (iii) you providing consent to the updated Terms in a specified manner, as applicable. Unless otherwise stated, your continued use of the Services constitutes your acceptance of such change(s). If you do not agree to any change(s) after receiving a notice of such change(s), then, notwithstanding anything to the contrary herein, your sole recourse is to terminate the Agreement, effective as of the end of the then current Initial Term or Renewal Term, by providing Tebra written notice of termination prior to your continued use of the Services. Please regularly check the Services to view the then-current Terms.

d) Feedback

If Customer provides feedback or suggestions about the Service, then Tebra (and those it allows to use its technology) may use such information without obligation to Customer.

e) Beta Features

i. If Customer is invited to access any beta features of the Service or a Customer accesses any beta features of the Service, Customer agrees that:
   - such features have not been made commercially available by Tebra;
   - such features may not operate properly, be in final form, or be fully functional;
   - such features may contain errors, design flaws, or other problems;
   - it may not be possible to make such features fully functional; use of such features may result in unexpected results, corruption or loss of data, or other unpredictable damage or loss;
   - such features may change and may not become generally available; and
   - Tebra is not obligated in any way to continue to provide or maintain such features for any purpose in providing the ongoing Service.

ii. These beta features are provided **AS IS, with all faults**. **Customer assumes all risk arising from use of such features, including, without limitation, the risk of damage to Customer's computer system or the corruption or loss of data.**

f) No Assignment

i. Tebra may assign or transfer the Customer Agreement (or its rights and/or obligations) to any third party without Customer's consent.

ii. Customer may not assign or transfer the Customer Agreement to a third party without the prior written consent of Tebra, except that the Customer Agreement may be assigned (without Tebra's consent but with notice) as part of a merger, or sale of all or substantially all of the business or assets, of Customer.

iii. The Customer Agreement will bind and inure to the benefit of each party's successors and permitted assigns.

g) Independent Contractors and Enforceability

i. The parties are independent contractors with respect to each other.

ii. If any term of the Customer Agreement is invalid or unenforceable, the other terms remain in effect.

h) Survival of Terms

All terms survive termination of the Customer Agreement that by their nature survive for a party to assert its rights and receive the protections of the Customer Agreement.

i) Customer Name

Tebra may use Customer's name and logo in customer lists and related promotional materials describing Customer as a customer of Tebra, which use must be in accordance with Customer's trademark guidelines and policies, if any, provided to Tebra. Customer may opt out of this provision by sending written notice to legal@tebra.com.

j) Force Majeure

Except for the obligation to pay money, neither party will be liable for any failure or delay in its performance under the Customer Agreement due to any cause beyond its reasonable control, including acts of war, acts of God, earthquake, flood, embargo, riot, sabotage, labor shortage or dispute, governmental act or failure of the Internet, provided that the delayed party:

i. gives the other party prompt notice of such cause, and
ii. uses its reasonable commercial efforts to correct promptly such failure or delay in performance.

k) Notice

i. Except as otherwise provided herein, any notice or communication required or permitted to be given hereunder may be delivered by hand, deposited with an overnight courier, sent by confirmed facsimile, or mailed by registered or certified mail, return receipt requested, postage prepaid to the address for the applicable party as furnished in writing by either party hereto to the other. Tebra's address for notice is: 1111 Bayside Drive, Corona Del Mar, CA 92625, Attn: General Counsel, and by email to: legal@tebra.com.
ii. Such notice will be deemed to have been given as of the date it is delivered, mailed or sent, whichever is earlier.

Updated effective June 1, 2023

Business Associate Agreement

This Business Associate Agreement (the "Agreement") shall be incorporated into the Terms of Service Agreement for Customers that are Covered Entities (as defined in the HIPAA Rules) and that provide Protected Health Information ("PHI") (as defined in the HIPAA Rules) to Tebra Technologies, Inc. and its subsidiaries ("Tebra" or "Business Associate") in connection with the software and services they have purchased.

Recitals

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), the U.S. Department of Health and Human Services issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") and Breach Notification Standards for Unsecured Protected Health Information (the "Breach Notification Rule") at 45 CFR parts 160 and 164 (collectively the "HIPAA Rules");

WHEREAS, in order to ensure that Covered Entity and Business Associate remain in compliance with the HIPAA Rules and other applicable federal and state laws and regulations regarding the disclosure of PHI to Business Associate, the parties have agreed to enter into this Agreement;

NOW THEREFORE, Covered Entity and Business Associate agree as follows:

1. **Definitions**
   Capitalized terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules, and if no such definition is provided in such rules, then the meaning shall be that given to such capitalized term in the Terms of Service Agreement to which this Agreement is incorporated.

2. **Tebra Obligations and Activities**
   The obligations and activities of the Business Associate, as required by the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information and Technology for Economic and Clinical Health ("HITECH Act") and in regulations promulgated thereunder, are as follows:

a. Business Associate agrees to not use or disclose Protected Health Information other than (i) as permitted or required by the Agreement or as Required by Law; or (ii) as otherwise authorized by Covered Entity.
b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.
c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
d. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware.
e. Business Associate agrees to ensure that any subcontractor that creates, receives, maintains, or transmits electronic PHI originating from the Covered Entity on behalf of the Business Associate, agrees to substantially the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
f. Business Associate agrees to provide access, at the request of Covered Entity to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in in a time and manner that allows Covered Entity to meet the requirements under 45 CFR § 164.524.
g. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity, in a time and manner that allows a Covered Entity to meet the requirements of 45 CFR 164.526 and in the time and manner of within thirty (30) days.
h. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary, for purposes of the Secretary determining compliance with the Privacy Rule.
i. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.
j. Upon request of Covered Entity, Business Associate agrees to provide to Covered Entity or an Individual, information collected in accordance with Section 2 (ix) of this Agreement, as necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

k. Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity in accordance with the 45 CFR 164.306 (the HIPAA Security standards).

l. Business Associate shall report to the Covered Entity any use or disclosure of PHI not permitted by this Agreement. Business Associate shall report any Breach of Unsecured PHI to Covered Entity in a manner that is in compliance with its obligations pursuant to 45 CFR §164.410.

m. Business Associate shall report a successful Security Incident in accordance with Section xii above and shall report unsuccessful Security Incidents upon request of Covered Entity.

n. When using, disclosing or requesting PHI, Business Associate agrees to use, disclose or request the minimal amount of information necessary for the stated purpose, unless an exception to the minimum necessary rule, as set forth in 45 CFR §164.502(b)(2).

3. **Permitted Uses and Disclosures**

The permitted uses and disclosures of the Business Associate, as required by the Health Insurance Portability and Accountability Act (HIPAA) and in regulations promulgated thereunder, are as follows:

a. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Terms of Services Agreement and this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and 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 the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).
d. Business Associate may use PHI to de-identify the information in accordance with 45 CFR 164.514(a)-(c), and shall retain any and all ownership claims relating to the de-identified data it creates from such PHI.
e. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

4. **Covered Entity's Obligations**
The obligations of Covered Entity, as required by HIPAA and in regulations promulgated thereunder, are as follow:
    a. To the extent that Covered Entity utilizes services provided by the Business Associate to communicate with patients, Covered Entity is responsible for obtaining and documenting authorizations or requests from patients to communicate through this service and to inform patient of risks associated with such communications as applicable. It shall be Covered Entity's responsibility to determine what permissions, authorizations or consents shall be documented and maintained for HIPAA compliance purposes. Business Associate does not obtain consent, authorization or permission from patients and the parties agree that is not Business Associate's obligation to do so or to document or maintain any consent, authorization or permission obtained from patients.
    b. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
    c. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
    d. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
    e. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

f. Covered Entity agrees to comply with the HIPAA Security Rule, including, without limitation, safeguarding all computers, laptops, cell phones, tablets, or other mobile devices in accordance with the HIPAA Security Regulations.

5. **Term and Termination**
   a. The term of this Agreement shall be effective as effective time contemplated by the Terms of Service Agreement to which this Agreement is incorporated, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions in this Section.
   b. Termination For Cause. In addition to any termination rights set forth in the Terms of Service Agreement, in the event of a material breach of this Agreement, the other party shall either: (i) provide the breaching party with an opportunity to cure the breach or end the violation, and terminate the Agreement (including this Agreement) if the breaching party does not cure the breach or end the violation within sixty (60) days, or (ii) immediately terminate the Terms of Service Agreement (and this Agreement) if cure is not possible.
   c. Termination upon Issuance of Guidance or Change In Law. If the Secretary provides additional guidance, clarification or interpretation on the Privacy Rule, or there is a change or supplement to the HIPAA statutes or regulations (both referred to as a "HIPAA Change"), such that a party hereto determines that the service relationship between Business Associate and Covered Entity is no longer a Business Associate relationship as defined in HIPAA, such party shall provide written notice to the other party of the HIPAA Change, and upon mutual agreement of the parties that the HIPAA Change renders this BA Agreement unnecessary, this Agreement shall terminate and be null and void.
   d. The respective rights and obligations of Business Associate under this Section 5 of this Agreement shall survive the termination of this Agreement for any reason.

6. **Other**
   a. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA Rules and the HIPAA.
   b. The parties agree that Business Associate may unilaterally amend this Agreement from time to time for the reasons set forth in the above paragraphs

and for other business reasons and that any such amended agreement which Business Associate signs on a later date will supersede this Agreement.

c. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Rules.
d. The terms Covered Entity and Business Associate are used in this Agreement only for purposes of convenience and are not meant to imply that either party would meet the definition of Covered Entity or Business Associate set forth in the HIPAA regulations.
e. To the extent not preempted by Federal law, this Agreement shall be governed and construed in accordance with the state laws governing the Terms of Service Agreement, without regard to conflicts of laws provisions that would require application of the law of another state.
f. This Agreement does not and is not intended to confer any rights or remedies upon any person other than the parties.
g. This Agreement supersedes and replaces any prior business associate agreements between the Covered Entity and Business Associate, including any of Tebra's subsidiaries as of the date set forth below.

IN WITNESS WHEREOF, the parties hereto have executed this Confidentiality Agreement as of the date of last signature below.

Covered Entity	**Business Associate**
	Tebra Technologies, Inc. (f/k/a Kareo, Inc.)
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

Platform Privacy Policy

Protecting your privacy on our platform

What this policy covers

This Platform Privacy Policy (**Policy**) pertains to the information about you that Tebra Technologies, Inc. (formerly known as Kareo, Inc.), including our subsidiary PatientPop, Inc. (**Tebra**, **we**, **us**, or **our**) collects, receives, uses, and shares from desktop, mobile, or cloud-based software via our Kareo Clinical (Electronic Health Records, or EHR), Kareo Billing (Practice Management), Kareo Engage, Kareo Telehealth, Kareo Cloud, or the Kareo Patient Portal (collectively, the **Platform**), or related customer support services (**Services**). It also describes the choices available to you regarding our use of your personal information and how you can access and update this information.

We may also provide different or additional privacy notices in connection with certain activities, programs, and offerings, including additional "just-in-time" notices that may supplement or clarify our privacy practices or provide you with additional choices regarding your personal information.

Personal information does not include publicly available information from government records, de-identified or aggregated consumer information, or information excluded from applicable laws, such as health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**). If you are a patient using our Platform, the information you provide to us through the Platform may be considered protected health information (**PHI**) and will be protected by Tebra as required by federal and state laws. Our processing of PHI on behalf of our healthcare provider customers is governed by our agreements with our customers, including our Business Associate Agreement as required by HIPAA. If you are a patient, your healthcare provider may also have its own privacy practices and policies that govern how your provider collects, uses, and shares your information.

This Policy does not cover information Tebra may collect or receive through our website, tebra.com, or any related services or applications (the **Site**). For more information about the information collected or received through our Site, please see our Website Privacy Policy.

This Policy does not cover the privacy practices of third parties. Our Site may include links to websites and/or applications operated and maintained by third parties. We have no control over the privacy practices of websites or applications that we do not own and cannot guarantee that such third parties will adhere to the same privacy practices as us. We strongly encourage you to review the privacy policies of those third parties.

Information We Collect

The types of personal information we obtain about you depends on how you interact with us and our services. When we use the term "personal information," it means information that identifies, relates to, describes, or can be associated with you. We may collect the following categories and specific types of personal information when you use our Platform:

Basic Identifiers

When you create an account on our Platform, we collect basic identifying information from you, including your full name, business address, email address, phone number, account name, signature, or

other similar identifiers. You may also provide personal information about other individuals, such as their name, email address and phone number. For example, if you choose to use our referral service to tell a colleague about our Site, we will ask for your colleague's name and email address to send a one-time email inviting your colleague to visit the Site. It is your responsibility to get permission from anyone whose personal information you provide to us. We will only use that personal information for the purpose of completing your request.

Government-Issued Identifiers

Depending on how you interact with us and what products or services you use on the Platform, we may collect information related to government-issued identifiers, including your driver's license number, or other similar government identifier for identification verification purposes. If you are a provider using our Platform, we will also collect your NPI or other credentials.

Payment Information

When you create an account, we will ask you to enter your credit card or ACH information.

Commercial Information

When you sign up for our services or request product information, we collect information related to the products or services you purchased or requested information about.

Professional Information

When you create an account on our Platform, we collect information related to your business, including your specialty, title, business address, and contact information.

Demographic Data

When you sign up for the Platform, we may collect information related to your gender, race, and ethnicity, some of which may include characteristics of protected classifications under state or federal law.

User Content

When you communicate with us, we collect information you provide to us, including emails, survey responses, comments, product reviews, testimonials, and other content.

Internet or Other Network Activity

Tebra may automatically receive and record information on our server logs from your browser, including your internet protocol (IP) address, your browsing or search history, and information related to your interactions with our Platform, emails, or advertisements.

Device Information and Other Unique Identifiers

We collect data about your device and how you and your device interact with our Platform, which may include your IP address, device identifiers, cookies, beacons, pixel tags, browser type, regional and language settings.

Usage and Performance Data

We collect data related to the use of our Platform. This may include your interactions with our Platform, error reports, and other data about the performance of our Platform. This data helps us to diagnose problems with our Site and to improve various features and solutions for your future use.

Geolocation Data

We may collect information, such as your IP address, that permits us to determine your general location (e.g., your city or state).

Sensory Information

We may record your voice or likeness, such as when you attend a live, online product demonstration or training session, or when we record customer service calls for quality assurance.

Inferences

We may also draw inferences from any of the information identified above.

How We Collect Information

Directly from You

We collect personal information you provide to us, such as when you create an account, contact us, respond to a survey, or sign up to receive emails, text messages, and/or postal mailings.

Using Cookies and Other Tracking Technologies

When you use certain portions of our Platform, open or click on emails we send you, or interact with our advertisements, we or third parties we work with automatically collect certain information using technologies such as cookies, web beacons, clear GIF, pixels, internet tags, web server logs, and other data collection tools. For more information, please see the Cookies and Other Tracking Technologies section below.

From Third Parties and Referral Partners

We obtain information from third parties that we have partnered with and other third parties we choose to collaborate or work with. For example, if you are referred to us by one of our billing company partners with whom you have a business relationship, we receive Basic Identifiers and Commercial Information from the billing company partner to contact you about the Platform.

From Social Media Platforms

If you interact with us on social media or use features, such as plugins, widgets, single sign-on, or other tools made available by social media platforms or networks (including Facebook, Twitter, Google, and LinkedIn) in connection with our Platform, we collect information that you, or the social media platform, share with us. For more information about the privacy practices of those social media platforms, please review the privacy policies and settings of the social media platforms and networks that you use.

From Other Sources

We may also obtain information about you from other sources, such as data analytics providers, marketing or advertising service providers, fraud prevention service providers, vendors that provide services on our behalf, or publicly available sources. We also create information based on our analysis of the information we have collected from you.

Cookies and Other Tracking Technologies

Certain portions of the Platform use cookies to recognize your preferences and temporarily store session information on your browser. A cookie is a small text file, which often includes an anonymous

unique identifier, that is placed on your computer's hard drive by a webpage server. Cookies contain information that can later be read by a web server in the domain that issued the cookie. We do link the information we store in cookies to personal information you submit while on our Platform.

Tebra uses both "session" cookies and "persistent" cookies. A session ID cookie will get removed automatically when you close your browser. We may use session cookies to make it easier for you to navigate our Platform. A persistent cookie remains on your hard drive for an extended period of time. We may also set a persistent cookie to store your passwords, so you don't have to enter it more than once if you so choose. We have cookies on our Platform but the data is only collected in the aggregate. We use a third-party tracking service that uses cookies and other tracking technologies to track non-personally identifiable information about visitors to our site in the aggregate. If you do not want the Platform to deploy cookies in your browser, you can set your browser to reject cookies or to notify you when a website tries to put a cookie in your browser software. You can also manually clear the cookies within your respective browser (for instructions, click here for Firefox; here for Chrome; and here for Safari). If you configure your browser to reject certain cookies, the opt-out may not function properly. If you change browsers or devices, or delete cookies, you may need to opt-out again.

Web Beacons/Gifs

Tebra uses software technology called clear gifs or Web beacons to help us better manage content on our Platform by informing us what content is effective. These technologies are tiny graphics with a unique identifier, similar in function to cookies, and are used to track the online movements of Web users. In contrast to cookies, which are stored on a user's computer hard drive, clear gifs are embedded invisibly on Web pages and are about the size of the period at the end of this sentence. In some cases, we tie information gathered by clear gifs to our customers' personal information; an example would be tracking emails that have been opened by recipients which allows us to measure the effectiveness of our communications and marketing campaigns.

Third Party Tracking

The use of cookies by a tracking utility company is not covered by our privacy policy. We do not have access or control over these cookies. Tracking utility company may use session ID cookies and/or persistent cookies.

We use Local Storage, such as HTML5, to store content information and preferences. Third parties with whom we partner to provide certain features on our website or to display advertising based upon your Web browsing activity also use HTML5 to collect and store information. Various browsers may offer their own management tools for removing HTML5.

Behavioral Targeting/Re-Targeting

We partner with a third-party ad network to either display advertising on our website or to manage our advertising on other sites. Our ad network partner uses cookies and Web beacons to collect information about your activities on this and other websites to provide you targeted advertising based upon your interests. If you wish to not have this information used for the purpose of serving you targeted ads, you may opt out of interest-based advertising across browsers and devices that participate in the Digital Advertising Alliance or Network Advertising Initiative by visiting their websites here and here, respectively. You may also opt out of interest-based advertising through the settings on your device or within a mobile app, but your opt-out preferences may apply only to the browser or device you are

using when you opt out. Please note this does not opt you out of being served advertising. You will continue to receive generic ads.

How We Use Your Information

We use the information we collect for the following purposes:

- **Providing Services**. For example, if you request a product demo and sign up for our services, we use the information you provided in your demo request to service and maintain your account, provide customer support, and communicate with you about our services.
- **Business Operations**. For our operational purposes and the operational purposes of our service providers and integration partners. This may include short-term, transient use, such as customizing content that we or our service providers display on the Site.
- **Core Functionality and Improvement**. We may use information we collect to provide core functionality on and to improve our Site, including for Site analytics.
- **Security, Safety, and Dispute Resolution**. We use collected information to protect the security and safety of our Site, including to detect bugs, report errors, and to detect, protect against, and prosecute security incidents and fraudulent or illegal activity.
- **Communicating With You**. We use your personal information to communicate with you and provide customer service and support. For example, we will send service-related announcements on rare occasions when it is necessary to do so, including if our Platform will be temporarily suspended for maintenance. We may also share updates about our products and services or provide relevant offers from third-party partners.
- **Marketing and Promotional Purposes**. We use personal information for marketing and promotional purposes, such as to send marketing, advertising, and promotional communications by email, text message or postal mail (such as promotions, new product launches, and referrals); and to show you advertisements for products and/or services tailored to your interests on social media and other websites.
- **Referrals**. If you choose to use our referral service to tell a colleague about our Site, we will ask for your colleague's name and business email address. We ask that you only provide this information after first obtaining your colleague's consent. We will automatically send your colleague a one-time email inviting him or her to visit the Site. Tebra stores this information for the sole purpose of sending this one-time email. Your colleague may contact us at privacy@tebra.com to request that we remove this information from our database.
- **Analytics and Personalization**. We use personal information to conduct research and analytics, including to improve our Platform, Services and product offerings; to understand how you interact with our Platform, advertisements, and communications with you to determine which of our products or services are the most popular, and to improve our Platform and marketing campaigns; to personalize your experience, to save you time when you use our Platform or visit our Site, and to customize the marketing and advertising that we show you; to understand how you use our Platform; to provide services, to better understand our customers' needs, and to provide personalized recommendations about our products and services.

- **Employment Decisions**. We use Job Applicant Information to make decisions about recruitment and in anticipation of a contract of employment. Providing this information is required for employment.
- **Legal Obligations**. We may provide access to your information, including personally identifiable information, when legally required to do so, including to comply with a court order, to cooperate with police investigations, or in connection with other legal proceedings.

Disclosed and Other Purposes. We may also use information for other purposes disclosed to you at the time we collect such information. For example, we obtain specific consent from customers prior to posting customer testimonials, comments and reviews on our Site which may contain personal information.

How We Share Your Information

In addition to the specific situations discussed elsewhere in this privacy policy, we disclose personal information in the following circumstances:

- **Corporate Affiliates**. We may share personal information with our corporate affiliates, including our parent company, sister companies and subsidiaries. Such corporate affiliates process personal information on our behalf as our service provider, where necessary to provide a product or service that you have requested, or in other circumstances with your consent or as permitted or required by law.
- **Legal Disclosures**. Tebra may be required to disclose personally identifiable information or PHI under special circumstances, such as to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service and related policies, or as otherwise required by law.
- **Service Providers**. We use service providers to perform services to support our core business functions and internal operations, including providing customer service to you via chatbot; sending postal mail, e-mails, and text messages; analyzing data; investigating fraudulent activity; conducting customer surveys. We may share personal information with such service providers as necessary for the third party to provide that service.
- **Business Partners**. With your consent, we do share your name and email with certain partners we may work with. If you would not like your information shared with these partners, notify us via **privacy@tebra.com**.
- **Third Parties**. We may share information with third parties, such as advertising networks, data analytics companies, Internet cookie information recipients, and social media networks. Our Platform has features such as plugins, widgets, and other features and tools made available by third parties that may result in information being collected or shared between us and the third party. For example, if you use Facebook's "Like" feature, Facebook may register the fact that you "liked" a product and may post that information on Facebook. You can also log in to portions of our Platform using sign-in services, such as LinkedIn Connect or an Open ID provider. These services will authenticate your identity and provide you with the option to share certain personal information with us, such as your name and email address, to pre-populate our sign-up

form. Services like LinkedIn Connect give you the option to post information about your activities on portions of our Platform to your profile page to share with others within your network. Please note that these other entities may independently collect information from or about you and the collection and use of your information by these entities is not governed by this Policy. Third party vendors, including Google, show our ads on sites on the Internet and use cookies to serve ads based on a user's prior visits to certain portions of our Platform. Users may opt out of Google's use of cookies by visiting the Google advertising opt-out page.

- **Transfers of Control**. We will transfer information about you if Tebra is acquired by or merged with another company. In this event, Tebra will notify you by email or by putting a prominent notice on our website before information about you is transferred and becomes subject to a different privacy policy.
- **Public Forums**. Some portions of our Platform provide the opportunity to post content in a public forum. If you decide to submit information in these public forums, that information will be publicly available.

In the last twelve months, we may have collected the following categories of personal information from or about you and may have disclosed or shared that information with certain categories of third parties for the purposes outlined below.

Categories of personal information collected	**Purposes for the collection or disclosure or personal information**	**Third parties with whom personal information may have been disclosed**
Basic Identifiers	• Providing the Service • Business operations • Communicating with You • Referrals • Business operations • With your consent • As required by applicable law	• Corporate Affiliates • Service Providers
Commercial Information	• Providing the Service • Business operations • Core Functionality and Improvement	• Corporate Affiliates • Service Providers

	• Security, Safety and Dispute Resolution • Marketing and Promotional Purposes • Referrals • Analytics and Personalization • As required by applicable law	
Professional Information	• Providing the Service • Business operations • Security, Safety and Dispute Resolution • Communicating with You • Marketing and Promotional Purposes • Referrals • Analytics and Personalization • Employment Decisions • As required by applicable law	• Corporate Affiliates • Service Providers
User Content	• Providing the Service • As required by applicable law	• Corporate Affiliates • Service Providers
Internet or Other Network Activity; Device Information and Other Unique Identifiers; Geolocation Data	• Providing the Service • Business operations • Core Functionality and Improvement	• Corporate Affiliates • Service Providers • Third Parties

	• Security, Safety and Dispute Resolution • Marketing and Promotional Purposes • Analytics and Personalization • As required by applicable law	
Usage and Performance Data	• Providing the Service • Business operations • Core Functionality and Improvement • Security, Safety and Dispute Resolution • As required by applicable law	• Corporate Affiliates • Service Providers
Sensory Information	• Providing the Service • As required by applicable law	• Corporate Affiliates • Service Providers

Additionally, if you are a healthcare provider or employee at a medical practice or billing company, we may have collected the following categories of personal information from or about you in the last twelve months and may have sold that information to certain categories of third parties for the purposes outlined below.

Categories of personal information collected	**Purposes for the collection and sharing or sale of personal information**	**Third parties with whom personal information may have been shared or sold**
Basic Identifiers	• With your consent (e.g., for business referrals)	• Business Partners

Commercial Information	• With your consent (e.g., for business referrals)	• Business Partners
Internet or Other Network Activity	• Marketing and Promotional Purposes • Analytics and Personalization	• Third Parties, like data analytics companies, social media companies, advertising networks, and cookie information recipients (e.g., Google)
Device Information and Other Unique Identifiers	• Marketing and Promotional Purposes • Analytics and Personalization	• Third Parties, like data analytics companies, social media companies, advertising networks, and cookie information recipients (e.g., Google)

Where We Store and Process Your Personal Information

Tebra Technologies, Inc. is based in the United States and uses service providers and has corporate affiliates that may be located outside of the United States.

If you submit personal information to us, your personal information may be processed in a foreign country, where privacy laws may be less stringent than the laws in the United States. By submitting your personal information to us, you agree to the transfer, storage, and processing of your personal information in a country other than your country of residence.

How We Protect Your Information

The security of your personal information is important to us. Personal information is maintained on our servers and those of our service providers, and may be accessible by authorized employees, representatives, and agents as necessary for the purposes described in this Policy.

While we follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, while we use reasonable and appropriate physical, electronic, and organizational safeguards to protect your personal information in our possession, we cannot guarantee its absolute security in all circumstances.

For more information about our security practices, please see our Security Notice. If you have any questions about security on our website, you can contact us at **privacy@tebra.com**.

Your Rights

Depending on your country or state of residence, you may be able to exercise the rights described below.

Accessing, Updating, Correcting, and Deleting Your Information

You may have the right to request access to and receive details about or a copy of the personal information we maintain or have processed about you, to update and correct inaccurate information, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. This section describes how to exercise those rights and our process for handling those requests, including our means of verifying your identity. If you would like further information regarding your legal rights under applicable law or would like to exercise any of them, please contact us here. While our contact form is the best way to reach us, you may also email us at privacy@tebra.com or call us at 844-422-7336.

- Access to Your Personal Information and Data Portability. You have the right to request that we disclose certain information to you about our collection and use of your personal information over the past 12 months. Once we receive your request and confirm your identity, we will disclose to you:
- The categories of personal information we collected about you and the sources from which we collected it.
- Our business or commercial purpose for collecting or selling that personal information.
- The categories of third parties with whom we share that personal information.
- If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
    - sales, identifying the personal information categories that each category of recipient purchased; and
    - disclosures for a business purpose, identifying the personal information categories that each category of recipient obtained.
- The specific pieces of personal information we collected about you (also called a data portability request).

You can submit a request to access or delete your personal information, or withdraw consent, by submitting a request through our contact form or calling 1-844-422-7336. We will retain your information for as long as your account is active or as needed to provide you services, comply with our legal obligations, resolve disputes, and enforce our agreements.

- Updates and Corrections to Your Personal Information. You can update your account by logging into your account, contacting our support team, or calling us at 1-844-422-7336. To update your personal information related to your employment at Tebra, please email us at privacy@tebra.com.
- Deletion of Your Personal Information. You have the right to request that we delete any of your personal information that we collected from you and retained, subject to certain exceptions. Once we receive your request and confirm your identity, we will review your request to see if an

exception allowing us to retain the information applies. We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, or otherwise perform our contract with you.
- Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- Debug products to identify and repair errors that impair existing intended functionality.
- Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law.
- Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- Comply with a legal obligation.
- Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

We will delete or de-identify personal information not subject to one of these exceptions from our records and will direct our service providers to take similar action.

Limiting the Use of Sensitive Personal Information

California residents have the right to limit the use of sensitive personal information. Tebra only collects sensitive personal information, such as your social security number, financial account information, and as otherwise defined by applicable law, when you provide it to us, such as in the job application process. We only use such sensitive personal information for the use disclosed at the time you provide it to us. Tebra does not use sensitive personal information for inferring characteristics about you.

Opting Out of Cookies and Sale/Sharing Using Online Tracking Technologies

Our use of online tracking technologies may be considered a sale or sharing under applicable law. As a visitor to our Site, you can opt out of being tracked by these third parties by clicking the "Do Not Sell My Personal Information" link at the bottom of our Site and selecting your preferences. Depending on your state of residence, you may also opt out by broadcasting an Opt-Out Preference Signal, such as the Global Privacy Control (GPC) (on the browsers and/or browser extensions that support such a signal). To

download and use a browser supporting the GPC browser signal, click here: https://globalprivacycontrol.org/orgs. If you choose to use the GPC signal, you will need to turn it on for each supported browser or browser extension you use.

Exercising Your Rights

You can submit a request to access, update, correct, or delete your personal information, or withdraw consent, by submitting a request through our contact form or by calling 1-844-422-7336.

You may only submit a request to know twice within a 12-month period. Your request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative, which may include your first and last name and email address.
- Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.

We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you.

Identity Verification

For security purposes, we may request additional information from you to verify your identity to enable us to process some requests. In such cases, we may contact you by email to verify your request. Depending on your request, we will ask for information such as your name and the email address associated with your Tebra account.

Authorized Agent

If you are a resident of California, Colorado, or Connecticut, you may designate an authorized agent to submit a request on your behalf to exercise your privacy rights described herein. To authorize an agent to do so, you must: (1) provide to such agent your signed permission to submit such request; and (2) verify your own identity directly with us. We may deny a request from an authorized agent if the agent does not provide adequate proof that they have been authorized by you to act on your behalf.

Responding to Requests

Upon receipt of your request, we will respond within the time frame permitted by the applicable law.

Appealing Requests

If you are a Colorado, Connecticut, or Virginia resident, you may appeal our decision to your request regarding your personal information. To do so, please contact us in any of the ways listed in the “Your Rights” section. We respond to all appeal requests as soon as we reasonably can, and no later than legally required.

Promotional Emails

To stop receiving promotional emails, you can click on the “unsubscribe” link at the bottom of any promotional email you receive from us. If you are a patient, please contact your healthcare provider to update your communication preferences.

Text Messages

To opt-out of receiving text messages from us, you can reply "STOP" to any text message you receive from us. If you are a patient, please contact your healthcare provider to update your communication preferences.

In-App Push Notifications

To stop receiving in-app push notifications from our mobile application, you can change your application settings on your mobile device.

Your Rights with Respect to Health and Medical Information We Collect or Process

If you are a patient of a healthcare provider who uses our Platform, we may collect or process information about you at the direction of your healthcare provider. If your healthcare provider is a Covered Entity under HIPAA, your rights with respect to your PHI are governed by HIPAA as well as our Business Associate Agreement with your healthcare provider. If you would no longer like to be contacted by that healthcare provider via our Platform, please contact your healthcare provider directly. If you would like to access or delete personal information, or to correct or update inaccurate personal information, please contact your healthcare provider directly to do so.

We will retain personal information we process on behalf of our customers for as long as needed to provide services to our customers. Tebra will retain this personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Data Aggregation Services & De-identified Data

To the extent we receive PHI from our customers that are Covered Entities under HIPAA, we may use such information to provide data aggregation services (as that term is defined by HIPAA) and to create de-identified data in accordance with 45 CFR 164.514(a)-(c) retaining all ownership claims relating to the de-identified data Tebra creates from PHI. Tebra may use, during and after this agreement, all aggregate non-identifiable information and de-identified data for purposes of enhancing the Service, technical support and other business purposes, all in compliance with the HIPAA Privacy Standards, including without limitation the limited data set and de-identification of information regulations.

Children's Privacy

Our Platform is not intended for or directed to children under the age of 18. We do not knowingly collect personal information directly from children under the age of 18 without parental consent. Children under 18 are not permitted to use the Platform and we do not knowingly allow individuals under the age of 18 to create accounts that allow access to our Platform. If we become aware that a child under the age of 18 has provided us with personal information, we will delete the information from our records.

Without limiting the above, the Platform does allow individuals over the age of 18 years—such as you, parents and guardians—to provide, share, and store personal information about others, including minors and children. Any user providing, storing, or submitting information on behalf of a child assumes full responsibility over the submission, use and transmission of such information.

We do not knowingly "sell," as that term is defined under the California Consumer Privacy Act, the personal information of minors under 16 years old who are California residents.

California Privacy Rights

California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our Site that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes. If you would like more information, please submit a written request to us at: Tebra Technologies, Inc., Attn: Legal, 1111 Bayside Drive, Corona Del Mar, CA 92625.

Changes to This Platform Privacy Policy

We may update this policy at any time for any reason. We encourage you to periodically review this page for the latest information on our privacy practices. We will provide additional notice to you if we make any changes that materially affect your privacy rights.

Questions

If you have questions or suggestions, you can contact us at:

Tebra Privacy
1111 Bayside Drive
Corona Del Mar, CA 92625
Phone: 888-775-2736
Email: privacy@tebra.com

Effective June 1, 2023.

Security Notice

How We Protect Your Data on Our Web-based Software Services

What This Security Notice Covers

This security notice pertains to the security measures in place at Tebra for protection of personal and protected health information in connection with the use of the Kareo web site, and the Kareo Billing, Kareo Clinical, Kareo Engage, Kareo Telehealth, Kareo Cloud, and Kareo mobile applications (collectively, the "**Service**").

Unique identification of users

To comply with the HIPAA requirements and to provide a secure service, Tebra requires all users to have a unique username. Tebra currently requires a valid email address to be the username for the Service.

In addition to a unique username, every user account must be protected with a password of sufficient complexity. Tebra allows its customers to set their own password complexity policy. If your user account has access to multiple Kareo customers, you will be required to use the more restrictive policy.

All Service sign-ins are protected by account lock-out systems. If a user incorrectly authenticates a number of times or the user's account is locked by a system administrator, their user account will be locked until a system administrator of the user's account unlocks it. Tebra's support team is prohibited from unlocking user accounts unless the account is the system administrator account.

Security on the Tebra web site

Service users may choose to sign into their account at the Kareo platform web site in order to access the downloads or account status. Such sign-ins are protected by TLS security. Your browser will usually display an indicator (such as a "lock" icon) when using a secure TLS connection.

Security in the Service

The Service communicates with secure Tebra-hosted and -controlled servers and networks. All communications are secured with public-key encryption. Tebra disallows the use of low cipher strength in our production service.

Tebra helps to ensure physical and technical security protections of customer data, as it uses servers located in SOC 2 type 2 certified hosting providers.

Tebra employs redundant, next-generation firewalls, intrusion detection and prevention services monitored 24X7X365. Critical servers are protected with industry-leading Endpoint Detection and Response protection. Tebra uses a PCI Approved Scanning Vendor ("**ASV**") as well as internal and external threat prevention delivering timely and accurate reports of our production services.

In addition to these controls, Tebra deploys up to date advanced threat protection services which help to identify, block, and track hacking attempts, scans, data breaches, adware, malware, spyware, Trojans, phishing attempts and other equally malicious requests.

Role-based security

Every user in the Service belongs to one or more roles. A role is defined by each customer and is assigned a set of permissions. Tebra roles follow an allow-then-deny pattern of applying permissions—such that multiple role permissions are combined, and then filtered against any role's restrictions.

Application locking

In accordance with HIPAA policies, the Service will automatically lock up if left unattended for a period of time. Correct credentials of the user will need to be provided prior to using the application again.

Tebra password policy

Tebra system passwords are meant to help protect sensitive patient medical and financial records, as well as practice financial information. They serve as a deterrent to malicious agents as well as protection against casual or accidental lowering of security through carelessness.

The passwords need to be at least (8) eight characters long and have to maintain a level of complexity such that they will not be easily guessed or cracked by a determined attacker.

A user may change their password at any point in the application or the Kareo platform web site. Passwords changed by third parties will immediately expire to allow users to log in but also to ensure that they immediately change their passwords to something that only they know.

Tebra will never store any passwords in permanent storage in a way that is reversible. The Service will never show the password in plain-text, human-readable form.

Strong Authentication

Enabling two-factor authentication ("**2FA**") is an additional layer of security that is recommended for all accounts. Only system administrators can enable 2FA. When 2FA is enabled, it is enabled at the account level and enabled for all users for all practices under the account.

Tebra's support team is prohibited from changing authentication settings unless the account is the system administrator account.

Changes to this security policy

Tebra may update this policy at any time for any reason. If there are any significant changes to how we handle security, we will make a reasonable commercial effort to send a notice to the contact email address specified in your company's Tebra account or by placing a prominent notice on our site.

Questions?

If you have questions or suggestions, you can contact us at:

Tebra Security Administrator
1111 Bayside Drive Suite 150
Corona Del Mar, CA 92625
security@tebra.com

To report a security violation, please call us at 888-77-KAREO (888-775-2736).
Last Updated: This policy was last updated on December 03, 2022.

Customer Support Policy

Support hours of operation and step-by-step instructions

Hours of Operation:

Mon-Fri, 5am-4pm (Pacific Time), excluding national holidays.

Scheduled Maintenance:

Scheduled maintenance may occur between 7pm-4am (Pacific Time), during weekends and holidays or with 24 hour notice.

How to Get Software Support for Tebra's solutions (including Kareo, PatientPop, and DoctorBase):

Step 1:	For legacy Kareo solutions (including DoctorBase), visit the Kareo Help Center to access how-to articles, video tutorials, feature guides, FAQs, the community forum and more.

For legacy PatientPop solutions, visit the PatientPop Help Center.

Step 2: If you cannot find your answer in the Kareo Help Center, choose one of the following options to contact Kareo customer Support:

- Email your questions using the web form here: Submit a Support Case
- Call 1-888-775-2736

If you cannot find your answer in the PatientPop Help Center, choose one of the following options to contact customer support:

- Email your questions using the web form here: Submit a Support Case
- Call 1-844-487-8399

How to Get Support For Kareo Billing Services:

Step 1:	If you have your biller’s direct contact information, please contact them directly.
Step 2:	If you do not have your biller’s direct contact information, call the Kareo Billing Service customer service line at 855-689-8166.

Pricing Policy

Pricing & Billing Policies for your Tebra Account

General Terms

Billing Frequency and Methods

Billing	Frequency and Method
Subscription fees	Billed monthly in advance
Transactional fees (electronic claims, eligibility checks, electronic remittance advice, paper claims, patient statements)	Billed monthly in arrears
Data storage fees	Billed monthly in arrears
Data import fees	Billed monthly in arrears
Professional services (training, credentialing)	Billed monthly in arrears
Onboarding fees	one-time fee; billed at sign up

- **Adding or Removing Providers.** New (activated) Providers will be charged on a pro-rata monthly basis, but removed (deactivated) Providers are charged for the last full month in advance.
- **Provider** *means* any provider of billable medical services to patients who is an employee, customer, or has an employment, contractor, or agent relationship with a Customer, for which the Service organizes information and provides clinical, billing, marketing, and managed billing services.
- **Physician Provider** *means* an *individual* Provider that is authorized to directly bill Medicare or commercial insurance companies for professional healthcare services rendered to patients, and holds a degree of, including but not limited to, DDS, DO, DMD, DPM, MD, ND, NMD, or OD.

- **Therapist** *means* any physical therapists (PT), occupational therapists (OT), speech language pathologists (SLP), marriage and family therapists (MFT), social worker (LCSW, MSW), psychologists.
- **Non-Physician Provider** *means* any *individual* Provider *other than a Physician Provider or Therapist*. This includes, but is not limited to, acupuncturists, audiologists, chiropractors, mid-wives, nurse practitioners, physician assistants or registered dieticians.
- **Supervising Provider** *means* a Physician Provider who monitors and aids Non-Physician Providers by signing/counter-signing notes, as well as prescribing medications. A Provider that has duties in addition to the foregoing shall not constitute a Supervising Provider.
- **Facility Provider** *means* an organization, facility, or lab that is authorized to directly bill Medicare or commercial insurance companies for institutional healthcare services rendered to patients.
- **Fees:** : All fees charged by Tebra are described in Tebra's Pricing Policy page and are determined by the subscription level selected and specific provider characteristics (example, Essentials, Plus, Pro, Physician or Non-Physician Provider, full-time or part- time, or specialty). All prices may change with 30 days electronic notice. You are responsible for keeping your email address updated with Tebra.
  Mailing fees (example, for mailings like paper insurance claims or paper patient statements) may be increased at any time to reflect a change in the USPS postage or processing costs.
- **Billing Transaction** *means* , in connection with subscription pricing based on billing transaction volume, any of the following: (i) electronic claims, (ii) eligibility checks and (iii) each request/claim submitted, paid and/or denied within an electronic remittance advice (ERA).

Billing & Other Terms

- **Account Changes:** Tebra bills on a calendar month basis starting on the 1st of the month. Account cancellations, terminations and other changes must be made ten (10) days prior to the end of the month in order for the changes to be reflected on your next invoice.
- **No Refunds/Credits:** All fees are nonrefundable and non-cancellable. Tebra does not refund or credit subscription fees for partial months, or any portion of a prepaid plan upon a deactivation of a Provider or account cancellation.

Customer is responsible for all fees (including any monthly minimum) for the entire term of the applicable order or subscription agreement.

- **Practices:** Must have at least one active Provider within a Practice for the Practice to remain active.
- **Minimum Fee:** There is a minimum monthly fee of $150 for any account that has not activated a Provider. When a Provider is activated, subscription fees will be charged accordingly.
- **Excess Claims by Facility Provider:** Tebra may modify the monthly fee after 30 days' notice if Customer exceeds 500 claims per month for any Facility Provider.
- **Tebra Platform:** Price is for the three module bundle of Tebra Clinical, Tebra Billing and Tebra Engage only. If one or more modules are canceled at any time, remaining modules revert to full price.
- **Multi-Practice Provider:** Providers activated within multiple practices within a single Tebra account will be charged one subscription fee, at the highest applicable subscription level (e.g., Essentials, Plus or Pro), subject to the Provider using and correctly inputting the same name, NPI, and other user information in connection with all relevant practices.
- **Reactivation Fee:** Tebra reserves the right to assess a $49 reactivation fee to Customers whose accounts are suspended based on late payments received more than fifteen (15) days following the payment due date.

Customer Support Plans & Fees

Phone, Email and Live Chat Support

- All subscription levels include unlimited access to customer support by email, live chat and phone.

Assisted Enrollment Service

- Assisted enrollment services include clearinghouse sign-up and setup of electronic services with insurance companies.
- Unlimited number of payers on your initial enrollment. Subsequent payers are not included.
- Assisted enrollments are included for all customers without additional fees.

Electronic Clearinghouse Services & Fees

Electronic Claims Submission (ANSI 837)

- Electronic claims submission service includes sending electronic claims in the ANSI 837 format to Tebra's Clearinghouse.
- $0.99 per electronic claim, per provider, per month for Low-Volume subscription plans beginning after the first 50 claims. No charge for other subscription levels.

Electronic Remittance Advice (ANSI 835)

- Electronic remittance advice service includes receiving electronic remittance advice messages from Tebra's Clearinghouse in the ANSI 835 format.
- No charge for all subscription levels.

Electronic Real-Time Insurance Eligibility Services (ANSI 270/271)

- Electronic real-time insurance eligibility services include performing electronic verification of insurance benefits from Tebra's Clearinghouse in the ANSI 270/271 format.
- No charge for all subscription levels.
- **Termination of Remittance Services:** In the event that Customer desires to discontinue electronic remittance services, then Customer must contact the insurance companies directly to request termination.

Paper Claims Mailing Services

Jopari (Workers Compensation and Auto Only) Paper Claims Mailing Services

- $0.99 for the first page, postage is included.
- $0.20 for each additional page.
- No fee for printing of paper claims to your own printer from Tebra.

Non-Jopari Clearinghouse Paper Claims Mailing Services

- $0.99 per paper claim printed and mailed, postage is included.
- No fee for printing paper claims to your own printer from Tebra.

Patient Payment Credit Card Services

Pricing	Per Transaction Fee
Credit Card Flat Rate	2.75% + $0.30
Processing Fee	Individual credit card payments above $5,000 will incur a 2% processing fee.

Patient Statement Mailing Service Fees

- Sending batches of patient statements to Tebra-affiliated processor for printing and mailing (postage is included).
- **First Page:** $0.99/statement.
- **Additional Pages:** $0.24/page.
- **Undeliverable Mail:** Statements rejected by the USPS as undeliverable are charged at the normal rate. A report with each reject and an explanation of the error will be provided so that address can be updated for future mailings.
- No fee for printing of patient statements to your own printer from Tebra.

Data Storage

- **Monthly Allowance:** For customers on Essentials, Plus, Pro, Platform, Standard, PT/OT/SLP, and Billing Company editions, each account is provided 250 gigabytes of data storage per Provider within the Practice. Any data storage that exceeds the amount provided will be billed at $0.15 per gigabyte monthly. For customers on other editions, please click here for data storage fees.

Data Import & Migration Fees

Data Import

- Data import is available for the following areas: Patient Demographics, Appointments, Patient Case (Insurance Policy), Payer List, Provider List, Service Locations, Patient Balances Forward, Scanned Documents (Clinical and Non-Clinical), Fee Schedule, and Care Summary Document (C-CDA).
- Fees for data imports are determined based on the data sets requested and volume of the specific import and are quoted through by Tebra's data services team.

Data Migration

- Moving practice data from a multi-practice account (e.g. a billing company) into a newly created customer account.
- May include all of the data within the practice, including but not limited to, patients, appointments, encounters, claims, payments, documents, settings, and clinical data.
- Permission: Requires written permission from the company administrator whose account the data originates.
- Fees for data migration are determined based on the details for the specific migration and are quoted through by Tebra's data services team.

What types of files can we accept data in?

Data Set	Format
Demographics	XLS, CSV
Insurance Companies, Plans, and Policy Info	XLS, CSV
Referring Providers	XLS, CSV
Service Locations	XLS, CSV
Fee Schedules	XLS, CSV
Service Locations	XLS, CSV
Appointments	XLS, CSV
Providers	XLS, CSV

Balance Forward	XLS, CSV
Fee Schedules	XLS, CSV
Journal Notes	XLS, CSV
Scanned Documents	PDF, doc, docx, gif, jpg, jpeg, html, png rtf, tif, txt
Clinical Document CCDA Discrete	XML

Robotic Process Automation Services Fees

Billing	**Frequency and Method**
Subscription fees	Billed monthly in advance on a per practice basis
Onboarding Fees	Billed in advance on a per practice basis
Transactional Fees (Smart Connector for HL7 & Patient Data; Automated Clinical Note Creation)	Billed monthly in arrears for each transaction/encounter above the standard monthly allotment
Transactional Fees (PDF Note Creation)	Billed monthly in arrears for each transaction

- Subscription Fees
    - ERA Processing: $85.00 per month per practice.
    - Un-Applied Payments: $65.00 per month per practice.

    - AR Courtesy Calls: $50.00 per month/ per practice for the first 150 minutes/texts; additional $0.20 per each minute/text above 150 minutes/texts.
- Transaction & Setup Fees:
    - Smart Connector for HL7 & Patient Data: $275.00 per month for the standard monthly transactions (2,000); $0.08/transaction above the standard monthly transactions.
    - Smart Connector for HL7 & Patient Data setup fee: $750 per practice for a single file or transaction feed.
    - Automated Clinical Note Creation: $0.10/encounter above the standard monthly clinical note encounters (2,000).
    - PDF Note Creation: $0.10/note.
    - A transaction consists of any appropriate patient and/or billing data for a single encounter.

Electronic Prescribing of Controlled Substances using Tebra EHR

- Tebra charges a one-time application fee for e-prescribing of controlled substances of $75.00.
- Prescription Drug Monitoring Program (PDMP) Add-On Service: (i) one-time implementation and setup fee of $500 per Facility; and (ii) $50/year per Authorized User

Fee Changes

- For Customers with month to month agreements, all fees may be changed with sixty (60) days' notice to Customer.
- For all Customers, Tebra reserves the right to increase its prices by no greater than 4.9% at any one time, no more frequently than once per 12 month period, upon thirty (30) days' notice to the Customer. This provision shall not apply to RPA customers.
- For all Customers, Tebra may increase fees to cover the cost of postage rate increases as well as regulatory, compliance, and other cost increases imposed by changes to applicable federal and state rules. Tebra will automatically apply the rate increase to all services impacted by the change with thirty (30) days' notice to the Customer.