Kareo customers can download a signed copy of this Business Associate Agreement at My Account

Business Associate Agreement

This Business Associate Agreement (the "**Agreement**") between Customer ("**Covered Entity**") and Kareo and its subsidiaries ("**Business Associate**") will be in effect during any such time period that Covered Entity has subscribed to and is using services provided by Kareo and/or its subsidiaries and upon termination as set forth in Section 5 of this Agreement.

Recitals

WHEREAS, Covered Entity has engaged Business Associate to perform services or provide software, or both;

WHEREAS, Covered Entity possesses Individually Identifiable Health Information that is protected under HIPAA (as hereinafter defined), the HIPAA Privacy Regulations (as hereinafter defined), the HIPAA Security Regulations (as hereinafter defined), and the HITECH Standards (as hereinafter defined) and is permitted to use or disclose such information only in accordance with such laws and regulations;

WHEREAS, Business Associate may receive such information from Covered Entity, or create and receive such information on behalf of Covered Entity, in order to perform certain of the services or provide certain of the goods, or both; and

WHEREAS, Covered Entity wishes to ensure that Business Associate will appropriately safeguard Individually Identifiable Health Information;

WHEREAS, Covered Entity and Business Associate agree as follows:

1. **Definitions**
   The parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in the HIPAA Privacy Regulations, the HIPAA Security Regulations, and the HITECH Standards (collectively the HIPAA Rules). Terms used in this agreement and not otherwise defined shall have the meaning of those terms in the HIPAA Rules.

   "Business Associate" shall have the same meaning as the definition for Business Associate set forth in 45 CFR 160.103.

   "Covered Entity" means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Privacy and HIPAA Security Regulations.

   "Data Aggregation" means, with respect to PHI created or received by a Business Associate in its capacity as the Business Associate of a Covered Entity, the combining of such PHI by the Business Associate with the PHI received by the Business Associate in its capacity as a

Business Associate of another Covered Entity, to permit data analyses that relate to the health care operations of the respective Covered Entities.

“Terms of Service Agreement” or TOS is the agreement between Kareo and its customers and end users. The TOS dictates the subscription terms and conditions, service level agreements and payment terms.

“Data Retention Period” is a designated time defined within the Kareo Terms of Service Agreement (TOS). Kareo will maintain the customer’s data containing ePHI for the defined period of time to allow the customer sufficient time to validate their downloaded data from the Kareo system. “Individually Identifiable Health Information” means information that is a subset of health information, including demographic information collected from an individual, and;

“Individually Identifiable Health Information” means information that is a subset of health information, including demographic information collected from an individual, and;

i. is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
ii. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for provision of health care to an individual; and
    a. that identifies the individual; or
    b. with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

“Individual” means the same meaning as the term “individual” in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

“Protected Health Information” or “PHI” has the same meaning as the term “protected health information” in 45 CFR § 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity and not including any unsolicited information received directly from an individual who is not yet a patient of Covered Entity (e.g., an individual who is using the Ask DoctorBase Service).

“Electronic Protected Health Information” or “ePHI” means the Protected Health Information that is transmitted by or maintained in electronic media as defined in the HIPAA Security Regulations.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

“HIPAA Privacy Regulations” means the regulations promulgated under the HIPAA by the United States Department of Health and Human Services to protect the privacy of Protected Health Information, including but not limited to, 45 CFR § 160 and 45 CFR § 164, Subpart A and E.

“HIPAA Security Regulations” means the regulations promulgated under HIPAA by the United States Department of Health and Human Services to protect the security of Electronic

Protected Health Information, including, but not limited to 45 CFR § 160 and 45 CFR § 164, Subpart A and C.

"HITECH Standards" means the privacy, security and security Breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and any regulations promulgated thereunder.

"Breach" shall mean the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under 45 CFR § 164, Subpart E (the "HIPAA Privacy Rule") "Breach" shall not include:

i. Any unintentional acquisition, access or use of Protected Health Information by a workforce member or person acting under the authority of Covered Entity or Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; or
ii. Any inadvertent disclosure by a person who is authorized to access Protected Health Information at Covered Entity or Business Associate to another person authorized to access Protected Health Information at Covered Entity or Business Associate, respectively, or organized health care arrangement in which Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or
iii. A disclosure of Protected Health Information where Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
iv. A Disclosure of Protected Health Information where a Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the factors set forth in 45 CFR 164.402 (2)(1)-(iv).

"Provider(s)" means any healthcare professional that provides billable 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 medical billing management.

"Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

"Secretary" means the Secretary of the United States of America Department of Health and Human Services or his designee.

2. 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:

i. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required by Law.
ii. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.
iii. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
iv. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.
v. Business Associate agrees to ensure that any subcontractor, that creates receives, maintains or transmits electronic protected health information originating from the Covered Entity on behalf of the Business Associate, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
vi. Business Associate agrees to provide access, at the request of Covered Entity to Protected Health Information 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.
vii. Business Associate agrees to make any amendment(s) to Protected Health Information 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.
viii. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information 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.
ix. Business Associate agrees to document such disclosures of Protected Health Information 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 Protected Health Information in accordance with 45 CFR § 164.528.
x. 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 Protected Health Information in accordance with 45 CFR § 164.528.
xi. Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information 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).
xii. Business Associate shall report to the Covered Entity any use or disclosure of Protected Health Information not permitted by this Agreement. Business Associate shall report any Breach of Unsecured Protected Health Information to Covered Entity in a manner that is in compliance with its obligations pursuant to 45 CFR §164.410.

xiii. 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.

xiv. When using, disclosing or requesting Protected Health Information, 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:

i. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information 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.

ii. Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information 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.

iii. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

iv. Business Associate may use Protected Health Information 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 Protected Health Information.

v. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with § 164.502(j)(1).

4. Obligations

The obligations of Covered Entity, as required by Health Insurance Portability and Accountability Act (HIPAA) and in regulations promulgated thereunder, are as follow:

i. 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.

ii. 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 Protected Health Information.

iii. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

iv. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information 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 Protected Health Information.

v. Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

vi. 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. Termination

i. Notwithstanding anything to the contrary stated in this Agreement, upon termination of this Agreement, for any reason, and after any Data Retention Period as is set forth in the Kareo Terms of Service Agreement between Business Associate and Covered Entity during which Business Associate may obtain copies of Protected Health Information, Business Associate shall destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

ii. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon determination that return or destruction of Protected Health Information is infeasible, or to the extent that Business Associate retains Protected Health Information for a Data Retention Period as set forth above in Section 5(i), Business Associate shall extend the protections of this Agreement to such Protected Health Information and, where applicable, limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

iii. 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

i. 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 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
ii. The parties agree that Business Associate may unilaterally amend this Agreement from time to time for the reasons set forth in the above paragraph and for other business reasons and that any such amended agreement which Business Associate signs on a later date will supersede this Agreement.
iii. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Rules.
iv. 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.
v. 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.
vi. This Agreement does not and is not intended to confer any rights or remedies upon any person other than the parties.
vii. This Agreement supersedes and replaces any prior business associate agreements between the Covered Entity and Business Associate, including any of Kareo's subsidiaries as of the date signed below.

Last Updated: February 29, 2020
To see previous versions, click here.
For the Terms of Service governing Kareo Managed Billing Customers, click here.