Cresta Intelligence, Inc.
Business Associate Agreement
(Updated June 2023)

This **BUSINESS ASSOCIATE AGREEMENT** ("**BAA**") is entered into as of the **Effective Date** (as defined in the Agreement), by Cresta Intelligence, Inc. ("Cresta") and the party entering into the Agreement with Cresta that refers to this BAA (the "**Customer**"). This BAA shall be deemed a part of the Agreement between Cresta and Customer governing the contractual relationship between Cresta and Customer, regardless of whether this document is signed. In the event of a conflict between the terms and conditions of this BAA and the Agreement, the terms and conditions of this BAA shall take precedence. All capitalized terms used in this Addendum and not defined in this Addendum shall have the meanings given to them in the Agreement.

1. **Definitions**

1.1. The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Business Associate, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information and Electronic Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

1.2. Except as the context of a provision dictates otherwise, a term used in this BAA and not defined in this Section or in the Agreement shall have the meaning given to it under HIPAA or HITECH, as applicable.

1.3. *Business Associate*. In reference to the party to this BAA, Business Associate shall mean Cresta, unless Customer is considered a Business Associate, in which case references to Business Associate shall mean Customer, and Cresta shall be considered a Subcontractor.

1.4. *Covered Entity*. In reference to the party to this BAA, Covered Entity shall mean Customer, unless Customer is considered a Business Associate, in which case references to a Covered Entity shall mean Customer's business customers covered by HIPAA.

1.5. *HIPAA* means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder relating to the privacy and security of Electronic Protected Health Information and breach notification, as amended.

1.6. *HITECH* means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and the regulations promulgated thereunder relating to the privacy and security of Electronic Protected Health Information, as amended.

1.7. *Privacy Rule* means the standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

1.8. *Security Rule* means the standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and C.

2. **Obligations and Activities of Cresta**

2.1. Cresta shall not use or disclose Electronic Protected Health Information other than as permitted or required by this BAA or as Required by Law.

2.2. Cresta will use appropriate physical, technical, and administrative safeguards to prevent the unauthorized use or disclosure of Electronic Protected Health Information. These safeguards shall include, but not be limited to, policies and procedures for reasonably and appropriately protecting the confidentiality, integrity, and availability of Electronic Protected Health Information. With respect to such information, Cresta shall meet the requirements of the Security Rule that apply to business associates.

2.3. Cresta will report in writing to Customer any use or disclosure of Electronic Protected Health Information not provided for by this BAA and any Security Incidents, of which it becomes aware. Notice is deemed provided, and no further notice will be given, with respect to routine unsuccessful attempts at unauthorized access to ePHI such as pings and other broadcast attacks on firewalls, denial of service attacks, failed login attempts, and port scans. Once per year, upon Customer's written request, Cresta will provide a summary of such unsuccessful Security Incidents, at an aggregate level. In the event of a Breach of Unsecured Protected Health Information by Cresta, Cresta shall notify Customer of the Breach in accordance with the requirements under 45 CFR § 164.410. Incidents under this section shall be reported without unreasonable delay

and in no case later than sixty (60) calendar days after discovery of the incident, unless a law enforcement delay applies pursuant to 45 CFR § 164.412. In the event of a law enforcement delay, Cresta shall notify Customer within the time frame required by such section.

2.4. Cresta will require any Subcontractor to agree to restrictions at least as strict as those that apply through this BAA to Cresta. Cresta may disclose all or some of the terms of this BAA to any of its Subcontractors to secure its compliance with such terms.

2.5. To the extent Cresta maintains Customer's Electronic Protected Health Information in its systems, in order to allow Customer to comply with the requirements under 45 CFR § 164.524 and/or 45 CFR § 164.526, as applicable, within fifteen calendar days of receiving a written request from Customer pursuant to a request by an Individual, Cresta shall provide Customer with Electronic Protected Health Information that Cresta maintains in a Designated Record Set for review or amendment.

2.6. Cresta will make internal practices, books, and records relating to the use and disclosure of Electronic Protected Health Information available to the Secretary in a time and manner designated by the Secretary, to allow the Secretary to determine Customer's compliance with the Privacy Rule.

2.7. Cresta will document disclosures of Electronic Protected Health Information and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of Electronic Protected Health Information in accordance with the requirements under 45 CFR § 164.528. Upon Customer's reasonable and timely request, Cresta shall provide Customer with such accounting within thirty (30) calendar days of receipt of notice of an Individual's request to allow Customer to comply with the requirements under 45 CFR § 164.528.

2.8. The Parties do not intend for Customer to delegate any HIPAA-regulated functions or obligations to Cresta.

2.9. Business associate may not use or disclose Electronic Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Customer except for the specific uses and disclosures set forth below in Sections 3(c) and (d).

3. **Permitted Uses and Disclosures by Cresta**

3.1. Except as otherwise limited in this BAA, Cresta may use or disclose Electronic Protected Health Information to:

(a) Perform obligations, functions, and activities as necessary to perform the services set forth by the Parties in the Agreement;

(b) Perform its obligations under this BAA;

(c) Conduct activities for its own proper management and administration or carry out its own legal responsibilities, provided that any disclosure of Electronic Protected Health Information for such purpose shall be either: (i) Required By Law; or (ii) made after Cresta obtains reasonable assurances from the recipient of the Electronic Protected Health Information that the Electronic Protected Health Information will be held confidentially, that it will be used and disclosed further only for the purpose for which it was disclosed to the recipient, and that the recipient will notify Cresta of any instances of which it becomes aware that the confidentiality of the Electronic Protected Health Information has been breached;

(d) Provide data aggregation services relating to the health care operations of Customer; and

(e) Report violations of law in accordance with 45 CFR § 164.502(j)(1).

4. **De-Identified Data**

Cresta may use Electronic Protected Health Information that is de-identified in accordance with 45 CFR § 164.514(a)-(c) for its own business purposes.

5. **Obligations of Customer**

5.1. Customer shall notify Cresta of:

(a) Any provisions in its notice of privacy practices prepared in accordance with 45 CFR § 164.520 that may affect

Cresta's responsibilities with respect to Electronic Protected Health Information and of any modifications thereto.

(b) (i) any restriction to the use or disclosure of Electronic Protected Health Information that Customer has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Cresta's use or disclosure of Electronic Protected Health Information; and (ii) any changes in, or revocation of, permission by an Individual to use or disclose Electronic Protected Health Information, to the extent that such changes may affect Cresta's use or disclosure of Electronic Protected Health Information.

5.2. Permissible Disclosures by Customer. Customer 1) will not provide Cresta more than the minimum Electronic Protected Health Information necessary for Cresta to perform functions that are permitted or required under this BAA and 2) will implement and apply physical, technical, and administrative safeguards to transmit Electronic Protected Health Information to Cresta in a manner that meets the requirements of HIPAA and HITECH, as applicable.

5.3. Necessary Consents. Customer shall obtain or have obtained all necessary authorizations, consents, and other permissions that may be required under applicable law to provide, whether directly or indirectly, Electronic Protected Health Information to Cresta.

5.4. Permissible Requests by Customer. Customer shall not request Cresta to use or disclose Electronic Protected Health Information in any manner that would not be permissible under HIPAA or HITECH if done by Customer.

6. **Term and Termination**

6.1. The term of this BAA shall begin as of the Effective Date and shall terminate as provided elsewhere in this BAA or when all of the Electronic Protected Health Information is destroyed or returned to Customer or its designee.

6.2. If Customer knows of a pattern of activity or practice by Cresta that constitutes a material breach or violation of Cresta's obligations under the BAA, Customer shall notify Cresta of the breach and of the reasonable period during which Cresta may take measures to cure the breach or end the violation. If Cresta does not cure the breach or end the violation within that period, Customer shall terminate this BAA and, the extent applicable, its Agreement with Cresta for the provision of services pertaining to Electronic Protected Health Information as soon as feasible.

6.3. Upon termination of this BAA, Cresta shall have the following obligations:

(a) Except as provided in Section 6.3(b), Cresta shall return or, at Customer's direction, destroy all Electronic Protected Health Information received from Customer, or created, maintained, or received by Cresta on behalf of Customer

(b) If Cresta determines that returning or destroying any Electronic Protected Health Information is infeasible, Cresta shall:

(i) Retain only that Electronic Protected Health Information which is necessary for Cresta to continue its proper management and administration or to carry out its legal responsibilities;

(ii) Return to Customer or destroy the remaining Electronic Protected Health Information that Cresta still maintains in any form;

(iii) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information to prevent use or disclosure of the information, other than as provided for in this section, for as long as Cresta retains the Electronic Protected Health Information;

(iv) Not use or disclose Electronic Protected Health Information retained by Cresta other than for the purposes for which such information was retained and subject to the same conditions set out at Sections 2 and 3 above which applied prior to termination; and

(v) Return to Customer or destroy the Electronic Protected Health Information retained by Cresta when it is no longer needed by Cresta for its proper management and administration or to carry out its legal responsibilities.

7. **Miscellaneous**

7.1. *Regulatory References*. A reference in this BAA to a section in HIPAA or HITECH, as applicable, means the section as in effect, as amended.

7.2. *Amendment*. The Parties will amend this BAA as necessary for the Parties to comply with the requirements of HIPAA or HITECH, as each may be amended or construed by courts of applicable jurisdiction or the Secretary. Each such amendment shall be made by and, unless the Parties mutually agree, effective as of the applicable compliance date for the change in rules or interpretation. The Parties may amend or terminate this BAA in a writing executed by authorized representatives of each Party.

7.3. *Communications*. Written communications from one Party to the other will be provided as set forth in the Agreement.

7.4. *Relationship*. With respect to all functions that Cresta performs on behalf of Customer that involve Electronic Protected Health Information, the Parties shall have no relationship other than that of independent contractors.

7.5. *Survival*. The rights and obligations of Cresta under Sections 6.3 of this BAA shall survive the termination of this BAA and the Agreement.

7.6. *Interpretation*. Any ambiguity in this BAA and the Agreement shall be resolved to permit Customer and Cresta to comply with their respective obligations under HIPAA and HITECH. In the event of any conflict between the provisions of this BAA and other provisions of the Agreement with regard to Electronic Protected Health Information, the provisions of this BAA shall govern.

7.8 *Integration*. This BAA constitutes the complete agreement between Customer and Cresta relating to the matters specified in this BAA and supersedes all prior representations or agreements, whether oral or written, with respect to such matters.

This BAA has been signed on behalf of each of the Parties by a duly authorized signatory.

CUSTOMER	**Cresta Intelligence, Inc.**
Signature	**Signature**
Name	**Name**
Title	**Title**
Date	**Date**