CITY OF Grand Junction COLORADO
PURCHASING DIVISION

**CITY OF GRAND JUNCTION, COLORADO**

# Business Associate Agreement

This Business Associate Agreement ("BAA") is entered into as of the ___ day of _____, [insert year], by and between the **City of Grand Junction**, Colorado, a Colorado home rule municipality located in Mesa County, Colorado ("Covered Entity" or "City"), and **[Insert Legal Entity Name]**, a [corporation/limited liability company/other entity type] organized and existing under the laws of the State of _____ ("Business Associate"). Covered Entity and Business Associate may be referred to individually as a "Party" and collectively as the "Parties."

## RECITALS

WHEREAS Covered Entity is a "covered entity" as defined by the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and implementing regulations at 45 C.F.R. Parts 160 and 164, as may be amended (collectively, "HIPAA");

WHEREAS, Covered Entity and Business Associate have entered or will enter, into one or more agreements pursuant to which Business Associate will provide certain services to Covered Entity (collectively, the "Underlying Agreement");

WHEREAS, while performing services under the Underlying Agreement, Business Associate may create, receive, maintain, or transmit Protected Health Information ("PHI"), as defined by HIPAA, on behalf of Covered Entity;

WHEREAS, by virtue of providing such services, Business Associate will qualify as a "business associate" of Covered Entity, as defined under HIPAA;

WHEREAS, both Parties acknowledge their mutual obligations to comply with HIPAA and other applicable federal and state laws concerning the privacy and security of PHI, including the HIPAA Privacy Rule (45 C.F.R. Part 160 and Subparts A and E of Part 164), the HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164), and the HIPAA Breach Notification Rule;

WHEREAS, the Parties are entering into this BAA to establish their respective duties and obligations regarding PHI and to support compliance with HIPAA and other applicable laws.

## AGREEMENT

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein, and the continued provision of Protected Health Information ("PHI") by Covered Entity to Business Associate under the Underlying Agreement in reliance on this BAA, the Parties agree as follows:

### 1. Definitions

All capitalized terms used in this BAA and not otherwise defined herein shall have the meanings ascribed to them by HIPAA, the HITECH Act, or applicable regulations.

**a.** "Affiliate" means a subsidiary or affiliate of Covered Entity that is, or has been, considered a covered entity, as defined by HIPAA.
**b.** "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI, as defined in 45 C.F.R. § 164.402.
**c.** "Breach Notification Rule" means the portion of HIPAA set forth in Subpart D of 45 C.F.R. Part 164.
**d.** "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, for purposes of this Agreement, shall refer to [Insert Legal Entity Name].
**e.** "Data Aggregation" means, with respect to PHI created or received by Business Associate in its capacity as the "business associate" under HIPAA of Covered Entity, the combining of such PHI by Business Associate with the PHI received by Business Associate in its capacity as a business associate of one or more other "covered entity" under HIPAA, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this BAA shall be consistent with the meaning given to that term in the Privacy Rule.
**f.** "Designated Record Set" has the meaning given to such term under the Privacy Rule, including 45 C.F.R. § 164.501.
**g.** "De-Identify" means to alter the PHI such that the resulting information meets the requirements described in 45 C.F.R. §§ 164.514(a) and (b).
**h.** "Electronic PHI" means any PHI maintained in or transmitted by electronic media as defined in 45 C.F.R. § 160.103.
**i.** "Health Care Operations" has the meaning given to that term in 45 C.F.R. § 164.501.
**j.** "HHS" means the U.S. Department of Health and Human Services.

**k.** "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.

**l.** "Individual" has the same meaning given to that term in 45 C.F.R. §§ 164.501 and 160.103 and includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

**m.** "Privacy Rule" means that portion of HIPAA set forth in 45 C.F.R. Part 160 and Part 164, Subparts A and E.

**n.** "Protected Health Information" or "PHI" has the meaning given to the term "protected health information" in 45 C.F.R. §§ 164.501 and 160.103, and it is limited to the information created or received by the Business Associate from or on behalf of the Covered Entity.

**o.** "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**p.** "Security Rule" means the Security Standards for the Protection of Electronic Health Information provided in 45 C.F.R. Part 160 and Part 164, Subparts A and C.

**q.** "Unsecured Protected Health Information" or "Unsecured PHI" means any "protected health information," as defined in 45 C.F.R. §§ 164.501 and 160.103, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS Secretary in guidance issued pursuant to the HITECH Act and codified at 42 U.S.C. § 17932(h).

## 2. Use and Disclosure of PHI

Business Associate shall use and disclose PHI only as permitted or required by this BAA, the Underlying Agreement, or as required by law. All uses and disclosures shall be limited to the minimum necessary to accomplish the intended purpose. Additional provisions include:

- Except as otherwise provided in this BAA, Business Associate may use or disclose PHI as reasonably necessary to provide the services described in the Agreement to Covered Entity, and to undertake other activities of Business Associate permitted or required of Business Associate by this BAA or as required by law.
- Except as otherwise limited by this BAA or federal or state law, Covered Entity authorizes Business Associate to use the PHI in its possession for the proper management and administration of Business Associate's business and to carry out its legal responsibilities. Business Associate may disclose PHI for its proper management and administration, provided that (i) the disclosures are required by law; or (ii) Business Associate obtains, in writing, prior to making any disclosure to a third party (a) reasonable assurances from this third party that the PHI will be

held confidential as provided under this BAA and used or further disclosed only as required by law or for the purpose for which it was disclosed to this third party and (b) an agreement from this third party to notify Business Associate immediately of any breaches of the confidentiality of the PHI, to the extent it has knowledge of the breach.

- Business Associate will not use or disclose PHI in a manner other than as provided in this BAA, as permitted under the Privacy Rule, or as required by law. Business Associate will use or disclose PHI, to the extent practicable, as a limited data set or limited to the minimum necessary amount of PHI to carry out the intended purpose of the use or disclosure, in accordance with Section 13405(b) of the HITECH Act (codified at 42 U.S.C. § 17935(b)) and any of the act's implementing regulations adopted by HHS, for each use or disclosure of PHI.
- Upon request, Business Associate will make available to Covered Entity any of Covered Entity's PHI that Business Associate or any of its agents or subcontractors have in their possession.
- Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).
- Business Associate shall not use PHI, in identifiable or de-identified form, to train, fine-tune, validate, or otherwise develop any artificial intelligence, machine learning, or large language model, whether for Business Associate's own use or for the benefit of any third party, without Covered Entity's prior written consent. This restriction applies regardless of whether the resulting model is made available to Covered Entity. Nothing in this Section restricts Business Associate's use of de-identified information created in accordance with 45 C.F.R. § 164.514(a) and (b) for purposes unrelated to AI/ML model development.

**3. Safeguards**

Business Associate shall implement and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of PHI, including Electronic PHI, that it creates, receives, maintains, or transmits on behalf of Covered Entity, in full compliance with the Security Rule. At a minimum, Business Associate shall: (a) encrypt all Electronic PHI at rest and in transit using encryption that meets or exceeds the standards specified in HHS guidance under Section 13402(h)(2) of the HITECH Act, including the use of FIPS 140-2 (or successor) validated cryptographic modules; (b) enforce multi-factor authentication for all remote and administrative access to systems containing PHI; (c) implement role-based access controls and the principle of least privilege, with access reviews conducted no less than annually; (d) maintain centralized logging and monitoring of access to PHI, with logs retained for no less than six (6) years; (e) conduct an annual risk assessment consistent with 45 C.F.R. § 164.308(a)(1)(ii)(A) and a vulnerability scan no less than quarterly, and conduct an independent penetration test of systems handling PHI no less than annually; (f) maintain a documented patch management program that remediates Critical and High severity

vulnerabilities within thirty (30) calendar days of identification; (g) maintain a documented incident response plan, tested no less than annually; (h) require workforce members with access to PHI to complete HIPAA privacy and security training upon hire and annually thereafter; and (i) conduct background checks on workforce members with access to PHI prior to granting such access, to the extent permitted by law. Business Associate shall take all reasonable steps, including the provision of adequate training to its employees, to ensure compliance with this BAA and to prevent actions or omissions by its workforce, agents, or subcontractors that would result in a breach of this BAA. Business Associate shall remain responsible for the acts and omissions of its workforce, agents, and subcontractors with respect to PHI.

**4. Reporting Obligations**

- I**mproper Use or Disclosure:** Business Associate shall notify Covered Entity, in writing, of any use or disclosure of Protected Health Information (PHI) not permitted by this BAA, applicable law, or the Underlying Agreement without unreasonable delay, and in no event later than forty-eight (48) hours after discovery by Business Associate, its workforce, agent, or subcontractor.
- **Security Incidents:** Business Associate shall notify Covered Entity of any Successful Security Incident, unauthorized access, cybersecurity event, or compromise involving PHI or Covered Entity data without unreasonable delay, and in no event later than forty-eight (48) hours after discovery by Business Associate, its workforce, agent, or subcontractor. For purposes of this Section, a "Successful Security Incident" means any Security Incident that resulted in unauthorized access to, use of, disclosure of, modification of, or destruction of PHI or Covered Entity data, or interference with system operations affecting PHI. Unsuccessful Security Incidents, including, without limitation, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service that do not result in a system being taken off-line, and malware that is detected and quarantined without access to PHI, shall be reported to Covered Entity on an aggregate basis no less than annually upon Covered Entity's request, and this Section shall constitute notice of the ongoing existence and occurrence of such Unsuccessful Security Incidents.
- **Breach Notification:** Business Associate shall notify Covered Entity of any Breach of Unsecured PHI in accordance with 45 C.F.R. Part 164, Subpart D, without unreasonable delay, and in no event later than ten (10) business days after discovery of the Breach. Such notice shall include, to the extent then known, the information required under 45 C.F.R. § 164.410(c), and shall be supplemented as additional information becomes available.
- **Cooperation and Mitigation:** Business Associate shall cooperate fully with Covered Entity in investigating, mitigating, responding to, documenting, and remediating any Security Incident, unauthorized disclosure, or Breach involving PHI or Covered Entity data.

- **Cost Reimbursement:** To the extent permitted by law and attributable to Business Associate's acts or omissions, Business Associate shall reimburse Covered Entity for reasonable costs, expenses, damages, notification obligations, regulatory penalties, mitigation expenses, credit monitoring services, and other remediation costs incurred by Covered Entity in responding to a Breach or Security Incident involving PHI or Covered Entity data.
- Insurance. Business Associate shall maintain, at its own expense and throughout the term of this BAA, cyber liability and privacy insurance with limits of not less than $2,000,000 per occurrence and $5,000,000 in the aggregate, covering first- and third-party losses arising from breaches of PHI or Covered Entity data, regulatory investigations and fines (to the extent insurable), notification costs, credit monitoring, forensic investigation, and business interruption. Business Associate shall name Covered Entity as an additional insured to the extent commercially available and shall provide Covered Entity with a certificate of insurance upon request and upon any material change in coverage.

## 5. Mitigation

Business Associate shall take reasonable and appropriate measures to mitigate, to the extent practicable, any known harmful effects resulting from any use, disclosure, Security Incident, or Breach involving PHI caused by Business Associate or its workforce, agents, subcontractors, or affiliates in violation of this BAA or applicable law.

## 6. Subcontractors and Agents

Business Associate shall ensure that any of its agents, subcontractors, or affiliates who have access to PHI, or to whom Business Associate provides PHI, first agree in writing to the same restrictions, conditions, and obligations concerning the use and disclosure of PHI as are imposed on Business Associate under this BAA. Each such agent or subcontractor shall also agree to implement reasonable and appropriate safeguards to protect the confidentiality, integrity, and availability of Electronic PHI created, received, maintained, or transmitted on behalf of Business Associate or, through Business Associate, on behalf of Covered Entity.

Business Associate shall obtain Covered Entity's prior written approval before engaging any agent or subcontractor that will create, receive, maintain, or transmit PHI on behalf of Business Associate. Covered Entity's approval shall not be unreasonably withheld, conditioned, or delayed. Business Associate shall maintain a current list of all approved subcontractors with access to PHI and shall provide such list to Covered Entity upon request. Business Associate shall notify Covered Entity in writing of any proposed change in approved subcontractors no less than thirty (30) calendar days prior to such change, and Covered Entity shall have the right to object to any such change on reasonable security or compliance grounds.

Business Associate shall remain fully responsible for the performance of its agents and subcontractors and shall ensure that all such subcontracts and agreements impose privacy and security obligations that are at least as stringent as those contained in this BAA.

Business Associate shall store, process, and access PHI solely within the United States, and shall not permit any agent, subcontractor, or workforce member located outside the United States to access PHI, without Covered Entity's prior written consent.

## 7. Audit Rights

Business Associate shall obtain and maintain, at its own expense, at least one of the following independent third-party audits or certifications covering systems used to create, receive, maintain, or transmit PHI: an independent HIPAA compliance report (AT-C 315), HITRUST CSF certification, or SOC 2 Type II report. Such audit or certification shall be renewed no less than annually and shall be current within the preceding twelve (12) months. Upon request, Business Associate shall provide Covered Entity, or any upstream Business Associate, with a copy of the most recent such report or certification. In addition, upon no less than thirty (30) calendar days' prior written notice, and no more frequently than annually (except following a Breach or Security Incident, in which case no notice or frequency limit shall apply), Covered Entity or its designated independent auditor shall have the right, at Covered Entity's expense, to inspect and audit Business Associate's facilities, systems, records, policies, and procedures relevant to its handling of PHI under this BAA, subject to reasonable confidentiality protections and Business Associate's reasonable security and access requirements.

Covered Entity agrees to maintain the confidentiality of any non-public audit documentation provided by Business Associate and shall not disclose such materials except as required by law.

## 8. Access, Amendment, and Accounting of Disclosures

Business Associate shall support Covered Entity in complying with its obligations regarding Individual rights under HIPAA, including:

- **Access (45 C.F.R. §164.524):** Furnishing copies of PHI maintained in a Designated Record Set.
- **Amendment (45 C.F.R. §164.526):** Amending PHI as directed by Covered Entity.
- **Accounting of Disclosures (45 C.F.R. §164.528):** Documenting disclosures and providing such information to Covered Entity as necessary.

Any direct requests received by the Business Associate from Individuals shall be promptly forwarded to the Covered Entity, within ten business days.

Any disclosure of, or decision not to disclose, the PHI requested by an Individual or a personal representative, and compliance with the requirements applicable to an Individual's right to obtain access to PHI shall be the sole responsibility of Covered Entity.

## 9. Books and Records

Business Associate shall make available its internal practices, books, records, policies, procedures, and other documentation relating to the use, disclosure, safeguarding, and protection of PHI to HHS, or as otherwise required by law, for purposes of determining compliance with HIPAA.

## 10. Responsibilities of Covered Entity

Regarding the use and/or disclosure of Protected Health Information by Business Associate, Covered Entity shall:

- Notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- Notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of PHI.
- Notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.
- Except for data aggregation or management and administrative activities of Business Associate, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity.

## 11. Ownership of Data

All PHI is and shall remain the sole property of Covered Entity. Business Associate shall have no ownership rights or other interest in PHI, except for such limited rights as necessary to perform its obligations under this BAA and the Underlying Agreement.

## 12. Indemnification

Business Associate shall indemnify, defend, and hold harmless Covered Entity, its directors, officers, employees, contractors and agents against any and all claims, losses, expenses, costs, damages, obligations, penalties, and liabilities which Covered Entity may incur by reason of Business Associate's breach of or failure to perform any of its obligations under this BAA.

## 13. Term and Termination

- This BAA will become effective on the date first written above and will continue in effect until all obligations of the Parties have been met under the Agreement and under this BAA.
- Covered Entity may immediately terminate this BAA, the Agreement, and any related agreements if Covered Entity determines that Business Associate has breached a material term of this BAA and Business Associate fails to cure the breach, to Covered Entity's reasonable satisfaction, within thirty (30) calendar days after receiving written notice from Covered Entity. If termination is not feasible, Covered Entity may report the issue to HHS.
- If Business Associate determines that Covered Entity has breached a material term of this BAA, Business Associate shall provide Covered Entity with written notice describing the breach and allow Covered Entity thirty (30) calendar days to cure the breach. Failure of Covered Entity to cure the breach within the applicable cure period may constitute grounds for termination of the Agreement and this BAA by Business Associate. Business Associate may report the issue to HHS.
- Upon termination of the Agreement or this BAA for any reason, and in any event within sixty (60) calendar days of such termination, all PHI maintained by Business Associate will be returned to Covered Entity in a mutually agreed format or destroyed by Business Associate using methods consistent with NIST Special Publication 800-88 (or successor guidance) such that the PHI is rendered unusable, unreadable, and indecipherable. Business Associate shall provide Covered Entity with a written certificate of destruction, signed by an authorized officer of Business Associate, identifying the PHI destroyed, the method of destruction, and the date of destruction. Business Associate will not retain any copies of such information. This provision will apply to PHI in possession of Business Associate's agents and subcontractors, and Business Associate shall be responsible for obtaining and delivering certificates of destruction from each such agent and subcontractor. If Business Associate determines in good faith that return or destruction of specified PHI is not feasible, Business Associate shall, within thirty (30) calendar days of termination, furnish Covered Entity with a written statement identifying the specific PHI for which return or destruction is infeasible and describing in reasonable detail the conditions that make return or destruction infeasible. Covered Entity's acceptance of such statement shall not be unreasonably withheld. Upon Covered Entity's written acceptance that return or destruction of specified PHI is infeasible, Business Associate will extend the protection of this BAA to such information for as long as Business Associate retains such information and will limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. The obligations set forth in this Section regarding the protection, return, destruction, and continued safeguarding of PHI shall survive termination of this BAA.

## 14. Effect of BAA

- This BAA is a part of and subject to the terms of the Agreement, except that to the extent any terms of this BAA conflict with any term of the Agreement, the terms of this BAA will govern.
- Except as expressly stated in this BAA or as provided by law, this BAA will not create any rights in favor of any third party.

## 15. Miscellaneous Provisions

- **Regulatory References.** A reference in this BAA to a section in HIPAA means the section as in effect or as amended at the time.
- **Notices.** All notices, requests, and demands, or other communications to be given under this BAA to a Party will be delivered by first-class mail, registered or certified mail, express courier, or electronic mail to the Party's address given below:

**A.** If to Covered Entity, to:

City of Grand Junction
Attn: Stevie Oviatt, Finance Supervisor
250 N 5th Street
Grand Junction, CO 81501

Telephone: 970-244-1538
Email: stevieo@gjcity.org

**B.** If to Business Associate, to:

[Insert Consultant Entity]
Attn: [Insert Contact Name, Title]
[Insert Address]
[Insert City, State, Zip Code]

Telephone: [Insert telephone number]
Email: [Insert email address]

- **Amendments and Waiver**. This BAA may not be modified, nor will any provision be waived or amended, except in writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.
- **HITECH Act Compliance.** The Parties acknowledge that the HITECH Act includes significant changes to the Privacy Rule and the Security Rule. The privacy subtitle of the HITECH Act sets forth provisions that significantly change the requirements

for business associates and the agreements between business associates and covered entities under HIPAA, and these changes may be further clarified in forthcoming regulations and guidance. Each Party agrees to comply with the applicable provisions of the HITECH Act and any HHS regulations issued with respect to the HITECH Act. The Parties also agree to negotiate in good faith to modify this BAA as reasonably necessary to comply with the HITECH Act and its regulations as they become effective, but, in the event that the Parties are unable to reach agreement on such a modification, either Party will have the right to terminate this BAA upon 30 days' prior written notice to the other Party.

IN WITNESS WHEREOF, the Parties have executed this Business Associate Agreement as of the dates set forth below.

COVERED ENTITY:

**CITY OF GRAND JUNCTION, COLORADO**

By: _____

Name: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE:

**[INSERT LEGAL ENTITY NAME]**

By: _____

Name: _____

Title: _____

Date: _____