CITY OF Grand Junction COLORADO
PURCHASING DIVISION

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "BAA") is made and entered into as of the ___ day of _____, **[insert year]**, by and between the **City of Grand Junction, Colorado**, a municipal government entity of the State of Colorado, located in the County of Mesa ("Covered Entity"), and **[Insert contractor/consultant]**, a [corporation/limited liability company/other entity type] duly 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 either a "covered entity" or a "business associate" of a covered entity, as those terms are 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 the regulations promulgated thereunder by the United States Department of Health and Human Services ("HHS"), all as codified at 45 C.F.R. Parts 160 and 164 (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 such term is defined under HIPAA.

WHEREAS, both Parties acknowledge its 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) and the HIPAA Security Rule (45 C.F.R. Part 160 and Subparts A and C of Part 164); and

WHEREAS, both Parties desire to enter into this BAA to establish its respective duties and responsibilities regarding PHI and ensure compliance with HIPAA and other applicable laws.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

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 CFR §164.402.

c. "Breach Notification Rule" means the portion of HIPAA set forth in Subpart D of 45 CFR Part 164.

d. "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.

e. "Designated Record Set" has the meaning given to such term under the Privacy Rule, including 45 CFR §164.501. B.

f. "De-Identify" means to alter the PHI such that the resulting information meets the requirements described in 45 CFR §§164.514(a) and (b).

g. "Electronic PHI" means any PHI maintained in or transmitted by electronic media as defined in 45 CFR §160.103.

h. "Health Care Operations" has the meaning given to that term in 45 CFR §164.501.

i. "HHS" means the U.S. Department of Health and Human Services.

j. "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.

k. "Individual" has the same meaning given to that term in 45 CFR §§164.501 and 160.130 and includes a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

l. "Privacy Rule" means that portion of HIPAA set forth in 45 CFR Part 160 and Part

164, Subparts A and E.

m. "Protected Health Information" or "PHI" has the meaning given to the term "protected health information" in 45 CFR §§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.

n. "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.

o. "Security Rule" means the Security Standards for the Protection of Electronic Health Information provided in 45 CFR Part 160 & Part 164, Subparts A and C.

p. "Unsecured Protected Health Information" or "Unsecured PHI" means any "protected health information" as defined in 45 CFR §§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 the guidance issued pursuant to the HITECH Act and codified at 42 USC §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 USC §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 CFR §164.502(j)(1).

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. 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 report to Covered Entity, in writing, any use or disclosure of PHI not permitted by this BAA within five (5) business days of discovery.

- **Security Incidents:** Business Associate shall report to Covered Entity any actual or suspected Security Incident within five (5) business days.

- **Breach Notification:** Business Associate shall notify Covered Entity of any Breach of Unsecured PHI without unreasonable delay, and in no event later than thirty (30) calendar days after discovery.

- **Cost Reimbursement:** Business Associate shall reimburse Covered Entity for all reasonable costs, expenses, and damages incurred by Covered Entity in complying with the requirements of Subpart D of 45 C.F.R. Part 164, to the extent such costs result from a Breach attributable to Business Associate.

5. Mitigation

Business Associate will take reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of any use or disclosure of PHI by

Business Associate or its agents or subcontractors in violation of the requirements of this BAA.

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 notify Covered Entity (or any upstream Business Associate, as applicable) of all subcontracts or agreements under which an agent or subcontractor will receive PHI as described in Section 1.M of this BAA. Such notification shall occur within thirty (30) calendar days of execution of the subcontract and may be satisfied by placement of such notice.

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.

7. Audit Rights

Business Associate shall require all subcontractors or agents who access PHI to agree, in writing, to the same restrictions and conditions imposed on Business Associate by this BAA. Business Associate shall provide Covered Entity with notice of such subcontractors and ensure equivalent protections of PHI

Upon request, Business Associate will provide Covered Entity, or upstream Business Associate, with a copy of its most recent independent HIPAA compliance report (AT-C 315), HITRUST certification, or other mutually agreed upon independent standards-based third-party audit report. Covered entity agrees not to re-disclose the Business Associate’s audit report.

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 practices, books, and records relating to the use and disclosure of PHI to the Secretary of 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 CFR §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 CFR §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. 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 terminate immediately this BAA, the Agreement, and any other related agreements if Covered Entity makes a determination that Business Associate has breached a material term of this BAA and Business Associate has failed to cure that material breach, to Covered Entity's reasonable satisfaction, within 30 days after written notice from Covered Entity. Covered Entity may report the problem to the Secretary of HHS if termination is not feasible.

- If Business Associate determines that Covered Entity has breached the material term of this BAA, then Business Associate will provide Covered Entity with written notice of the existence of the breach and shall provide Covered Entity with 30 days to cure the breach. Covered Entity's failure to cure the breach within the 30-day period will be grounds for immediate termination of the Agreement and this BAA by Business Associate. Business Associate may report the breach to HHS.

- Upon termination of the Agreement or this BAA for any reason, all PHI maintained by Business Associate will be returned to Covered Entity or destroyed by Business Associate. Business Associate will not retain any copies of such information. This provision will apply to PHI in the possession of Business Associate's agents and subcontractors. If return or destruction of the PHI is not feasible, in the Business Associate's reasonable judgment, the Business Associate will furnish the Covered Entity with notification, in writing, of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return, or destruction of the 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 Parties understand that this Section 14.D. will survive any termination of this BAA.

13. 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.

14. 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 made via either first-class mail, registered or certified, or express courier, or electronic mail to the Party's address given below:

A. If to Covered Entity, to:

City of Grand Junction
Attn: Finance, Brandon Hinze
250 N 5th St
Grand Junction, CO 81501
T: 970-256-4046
E: brandonhin@gjcity.org

B. If to Business Associate, to:

[Insert Consultant Entity]
Attn: [Insert Contact Name, Title]
[Insert Address]
[Insert City, State, Zip Code]
T: [Insert telephone number]
E: [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.

The remainder of this page has been intentionally left blank