EXHIBIT C

HIPAA BUSINESS ASSOCIATE ADDENDUM

A. **Introduction.** The City (hereinafter the "Covered Entity") will make available and/or transfer to the Consultant (hereinafter the "Business Associate") certain information that is confidential and must be afforded special treatment and protection so Business Associate may perform services for Covered Entity pursuant to this Agreement (hereinafter the "Services Agreement"). Business Associate agrees that such information shall constitute Protected Health Information and can be Used or Disclosed only in accordance with this Addendum and a collection of federal laws, rules and regulations, including but not limited to, the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C. and 42 U.S.C.) ("HIPAA") Privacy Rule and Security Rule, the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§17921-17954 ("HITECH Act"), the Omnibus HIPAA Final Rule (78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified in scattered sections of 45 C.F.R. Parts 160 and 164)) ("Omnibus Rule") (collectively these federal rules are referred to collectively in this Addendum as the "HIPAA Rules") and applicable state and federal laws, rules and regulations regarding the privacy, confidentiality and security of specific types of health information.

The Consultant is a "Business Associate" under the Privacy and Security Rules and performs certain administrative services for or on behalf of Covered Entity which involves access to and the disclosure of Protected Health Information.

B. **Definitions**. For the purposes of this Addendum, the following terms shall have the following meaning:

1. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, as enacted in the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§17921-17954. All references to the "HITECH Act" in this Addendum shall be deemed to include the Omnibus Rule.

2. "Privacy Rule" means the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E as amended, clarified and supplemented from time to time. All references to the "Privacy Rule" in this Addendum shall be deemed to include the Omnibus Rule.

3. "Security Rule" means the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Part 160 and Part 164, Subparts A and C as amended, clarified and supplemented from time-to-time. All references to the "Privacy Rule" in this Addendum shall be deemed to include the Omnibus Rule.

4. "Standard Transactions Rule" means the HIPAA Standards for Electronic Transactions at 45 C.F.R. Parts 160 and 162.

5. The following terms used in this Addendum shall have the same meaning ascribed to them in the HIPAA Rules: Access, Breach, Business Associate, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Electronic Protected Health Information ("Electronic PHI"), Genetic Information, Individual, Individually Identifiable Health Information, Marketing, Minimum Necessary, Notice of Privacy Practices, Personal Health Records, Protected Health Information ("PHI"), Required By Law, Secretary, Security Incident, Business Associate, Unsecured Protected Health Information ("Unsecured PHI"), Use, Payment and Treatment. For purposes of this Addendum, unless otherwise specified, all obligations of Business Associate relating to PHI also shall apply to Electronic PHI.

C. **Nature of Use and Disclosure of Information**. Business Associate shall be permitted to Use and/or Disclose PHI provided or made available from Covered Entity solely to provide the services set forth in the Services Agreement and as specifically set forth in this Section C. Business Associate shall not Use or Disclose the PHI provided or made available by Covered Entity for any purpose other than as: (1) expressly permitted by this Addendum or the Services Agreement; (2) as Required By Law; (3) permitted with Covered Entity's prior written consent; (4) necessary to Business Associate's employees, agents or representatives who need to know such PHI for the purposes set forth in the Services Agreement; (5) to carry out Business Associate's legal responsibilities; or (6) for Data Aggregation for Covered Entity's Health Care Operations purposes. Furthermore, Business Associate may not Use or Disclose PHI in a manner that would violate 45 C.F.R. Part 164, Subpart E if done by Covered Entity.

D. **Business Associate's Obligations**.

1. Limits On Use And Disclosure. Business Associate agrees that the PHI provided or made available by Covered Entity shall not be Used or Disclosed other than as specifically set forth in Section C of this Addendum.

2. Appropriate Safeguards. Business Associate shall establish and maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of PHI and Electronic PHI and to prevent any use or disclosure of the PHI other than as provided in Section C of this Addendum.

3. Compliance with Security Rule. Business Associate shall comply with the Security Rule. Upon request by Covered Entity and not more than once annually, Business Associate shall provide Covered Entity with electronic or paper copies of its policies and procedures evidencing its compliance with the Security Rule.

4. Breach Reports. Following completion of its internal investigation, Business Associate shall report to Covered Entity, any of the following events (collectively referred to in this paragraph as "Breach"): (a) any Use or Disclosure of PHI not permitted under by Section C of this Addendum or permitted by law; (b) any Security Incident as defined in 45 C.F.R. §164.304; (c) any "breach of the security of the system" as defined in New York General Business Law Section 899-aa(1)(c); and (d) any Breach of Unsecured PHI as defined at 42 U.S.C. §§17921 and 17932(h) and 45 C.F.R. §164.402. Business Associate's written report shall:

(i) identify the nature of the non-permitted Access, Use or Disclosure, including the date of the Breach and the date of discovery of the Breach;

(ii) identify the PHI Accessed, Used or Disclosed as part of the Breach;

(iii) upon request, assist Covered Entity in the performance of a risk assessment concerning the Breach;

(iv) identify what corrective action Business Associate took or will take to prevent further non-permitted Access, Use or Disclosure;

(v) identify what Business Associate did or will do to mitigate any harmful effect(s) of the non-permitted Access, Use or Disclosure;

(vi) provide such other information as Covered Entity may require to supplement Business Associate's written report;

(vii) cooperate with Covered Entity in its efforts to mitigate the Breach and comply with the HIPAA Rules and any applicable state breach notification rules; and

(viii) provide such other information as may be required pursuant to subsequently issued regulations issued under the HIPAA Rules.

5. Right of Access to Information & Amendments. If Covered Entity provides Business Associate with PHI that is part of a Designated Record Set, within fifteen (15) days of Covered Entity's request, Business Associate agrees: (a) to provide access to such PHI to Covered Entity or, when directed by Covered Entity, to an Individual in order for Covered Entity to meet the access to information provisions of the Privacy Rule, including providing access to PHI in electronic form (if readily producible) under 45 C.F.R. §164.524 (c)(2) and (b) to make any amendments(s) to such PHI.

6. Providing Accounting. Under the Privacy Rule, Covered Entity must provide Individuals an accounting of certain Disclosures of their PHI for a reason other than Treatment, Payment and Health Care Operations. To assist Covered Entity in providing this information to Individuals, Business Associate agrees to document Disclosures of PHI and information related to such Disclosures for reasons other than Treatment, Payment and Health Care Operations during the Term of the Agreement to enable Covered Entity to respond to an Individual's request for an accounting of disclosures of PHI and make available such information to Covered Entity within ten days of Covered Entity's request for the information. If Business Associate (or its agents or subcontractors, if applicable) receives a request for an accounting of disclosures directly from an Individual, Business Associate shall forward such request to Covered Entity within fifteen (15) days of receipt. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested.

7. Audits By the Secretary. Business Associate agrees: (a) to make its internal practices, books and records relating to the Use or Disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Rules; (b) to cooperate fully with Covered Entity when responding to such regulatory audits and investigations; and (c) to concurrently provide Covered Entity with copies of the information it provides to the Secretary.

8. Additional Business Associate(s). Business Associate shall enter into a written agreement to ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to such PHI. If the agreement entered into between Business Associate and its subcontractors(s) permits additional subcontracting, Business Associate shall ensure that its subcontractor requires its subcontractors to agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to such PHI.

9. Minimum Necessary. Business Associate warrants, on its behalf and on behalf of its subcontractors, if any, that it will only request and use the minimum amount of PHI necessary to perform the stated purpose(s) of the Services Agreement as set forth in Section C of this Addendum.

E. **Additional Business Associate Obligations.**

1. Mitigation Procedures. Business Associate shall mitigate to the maximum extent, any harmful effect(s) arising out of or from the intentional or inadvertent Use or Disclosure of PHI that is or could be contrary to this Addendum, the HIPAA Rules or that could damage third parties.

2. Sanctions. Business Associate shall develop, implement and maintain sanction procedures for any employee, subcontractor agent who violates the terms of this Addendum or the HIPAA Rules. Such sanction procedures shall be made available to Covered Entity within fifteen (15) days of its reasonable request during the term of the Services Agreement or with fifteen (15) days of Covered Entity's request in the event of a Breach as set forth in Section D (4) of this Addendum.

3. Indemnification. The indemnification provisions of the Services Agreement shall apply to any breach of this Addendum.

4. Property Rights. The PHI shall be and remain the property of Covered Entity. Neither Business Associate nor its subcontractor(s), if any, shall acquire title or rights to the PHI, excluding any de-identified information, as a result of this Addendum or the Services Agreement, unless such PHI also include proprietary information of Business Associate.

5. Response to Government Authorities. Business Associate shall notify Covered Entity within fifteen (15) business days of receipt of a governmental or administrative subpoena(s) or any informal request(s) from a governmental entity relating in any way to the PHI provided pursuant to this Addendum and allow Covered Entity to seek a protective order or otherwise challenge the subpoena or request before responding thereto.

6. No Sale of PHI. Business Associate shall not directly or indirectly receive financial or in-kind remuneration in exchange for any PHI in compliance with 45 C.F.R. §164.502(a)(5)(ii).

7. Marketing. Business Associate shall not make or cause to be made any marketing communications about its products or services that is prohibited by 42 U.S.C. §17936(a) or 45 C.F.R. §164.508(a)(3).

8. Fundraising. Business Associate shall not make or cause to be made any written fundraising communication that is prohibited by 45 C.F.R. §164.514(f).

9. Restriction Requests. If applicable, Business Associate shall abide by any restriction request agreed to by Covered Entity under 45 C.F.R. §164.522(a) within fifteen (15) business days of receiving notice of such by Covered Entity.

10. Confidential Communications. If applicable, Business Associate shall abide by any confidential communication requirements that Covered Entity is subject to under 45 C.F.R. §164.522(b) within fifteen (15) business days of receiving notice of such by Covered Entity.

11. Genetic Information. If applicable, Business Associate shall not Use or Disclose PHI that is Genetic Information for underwriting purposes, as defined at 45 C.F.R. §164.502(a)(5), conducted on behalf of Covered Entity.

12. No Offshoring of PHI. Neither Business Associate nor its subcontractor(s), if any, shall provide the services contemplated under the attached agreement or Access, Use and Disclose any PHI outside of the Continental United States unless Covered Entity provides its express written consent, which may be unreasonably withheld.

13. Audits, Inspection and Enforcement. Within fifteen (15) days of a written request by Covered Entity, Business Associate and its agents or subcontractors, if any, shall allow Covered Entity to conduct a reasonable inspection of its facilities, systems, books, records, agreements, policies and procedures relating to the Use or Disclosure of PHI and the implementation of appropriate security safeguards pursuant to this Agreement for the purpose of determining whether Business Associate has complied with this Addendum; provided, however, that: (a) Business Associate and Covered Entity shall mutually agree in advance upon the scope, timing and location of such an inspection; (b) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection; (c) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate; and (d) such inspection shall not occur more than once annually or, in the event of a Breach described in Section D (4) of this Addendum, within thirty days of the Breach in question. The fact that Covered Entity inspects, or fails to inspect, Business Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Business Associate of its responsibility to comply with this Addendum, nor does Covered Entity's: (i) failure to detect; or (ii) detection, but failure to notify Business Associate or require Business Associate's remediation

of any unsatisfactory practices, constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this Agreement.

14. Standard Transactions. If Business Associate conducts in whole or in part Standard Transactions for or on behalf of Covered Entity, Business Associate shall comply with the Standard Transaction Rule.

15. De-Identified Information. Business Associate may store, analyze, access and use components of PHI that have been de-identified in accordance with 45 C.F.R. §164.514 and that do not contain any PHI or Individually Identifiable Health Information, provided that any such use is consistent with applicable law.

F. **Term and Termination.**

1. Term. This Addendum shall become effective on the Effective Date of the Services Agreement and shall continue until terminated by Covered Entity or the Services Agreement expires or is terminated. In addition, certain provisions and requirements of this Addendum shall survive its expiration or other termination of this Addendum as noted herein.

2. Material Breach. A breach by Business Associate of any material provision of this Addendum, as determined by Covered Entity, shall constitute a material breach and shall provide grounds for immediate termination of the Agreement by Covered Entity.

3. Reasonable Steps to Cure Breach. If Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of Business Associate's obligations under the HIPAA Rules or the provisions of this Addendum and does not terminate the Addendum, then Business Associate shall take reasonable steps to cure such breach or end such violation, as applicable. If Business Associate's efforts to cure such breach or end such violation are unsuccessful, Covered Entity shall either: (a) terminate this Addendum and the Services Agreement, if feasible; or (b) if termination of the Addendum and the Services Agreement is not feasible, Covered Entity shall report Business Associate's breach or violation to the Secretary. The obligations set forth in this Section are reciprocal and shall apply to Business Associate if it knows of a pattern of activity or practice of Covered Entity that constitutes a violation of Covered Entity's obligations under the HIPAA Rules and Business Associate shall cause this obligation to apply to its subcontractors, if permitted under the Services Agreement.

4. Judicial or Administrative Proceedings. Either party may terminate this Addendum and the Agreement, effective immediately, if: (a) the other party is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules or applicable state law; or (b) a finding or stipulation that the other party has violated any standard or requirement of the HIPAA Rules or applicable state laws is made in any administrative or civil proceeding in which the party has been named.

5. Effect of Termination. Upon termination of this Addendum for any reason, Business Associate shall return or destroy all PHI that Business Associate or its agents or subcontractors, if any, still maintain in any form and shall retain no copies of such PHI. If return

or destruction is not feasible, Business Associate shall continue to extend the protections of Sections C, D and E of this Addendum to such PHI, limit further Use of such PHI to those purposes that make the return or destruction of such PHI infeasible and retain such PHI for six years from the date this Addendum terminates. If Business Associate elects to destroy the PHI, Business Associate shall cause one of its authorized corporate officers to certify in writing to Covered Entity that such PHI has been destroyed. This provision shall survive the termination of this Addendum for any reason.

G. **Miscellaneous.**

1. Amendments. Any amendment to this Addendum needed to comply with the HIPAA Rules, shall be adopted automatically, without need for the parties' signatures, and deemed incorporated into this Addendum as of the compliance date of the applicable HIPAA Rules.

2. Ambiguity. Any ambiguities in this Addendum or its defined terms shall be resolved in favor of a meaning that promotes the parties' compliance with the HIPAA Rules.

3. Survival. The confidentiality and security obligations hereunder are perpetual and shall survive the termination of the Services Agreement or this Addendum for any reason.

4. Disclaimer. Each party is solely responsible for all decisions it makes regarding the Use, Disclosure and safeguarding of PHI.

5. No Agency. The parties agree and acknowledge that Business Associate is an independent contractor and it is not the intention of either party, whether expressed or implied, to create an agency relationship under the Federal Common Law of Agency.