

QHRC Business Associate Agreement*



This Business Associate Agreement (“Agreement”) is effective as of October 1, 2013 (the “Effective Date”) between _____ (“Covered Entity”) and Qualitative Health Research Consultants, LLC, (“Business Associate”).

WHEREAS, Business Associate may have access to protected health information in connection with Business Associate’s performance of services for Covered Entity.

WHEREAS, the parties wish to ensure the confidentiality of protected health information in accordance with applicable law, including, without limitation, HIPAA, the HIPAA Regulations and the HITECH Standards.

NOW, THEREFORE, the parties agree as follows:

1) Definitions. Any capitalized terms used, but not otherwise defined, in this Agreement will have the same meaning as those terms have under HIPAA, the HIPAA Regulations and/or the HITECH Standards.

a) “*Breach*” means the unauthorized acquisition, access, use, or disclosure of Protected Health Information (“PHI”) that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. “*Breach*” will not include:

(i) any unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of Covered Entity or Business Associate, as long as such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual with Covered Entity or Business Associate and such information is not further acquired, accessed, used, or disclosed by any person; or

(ii) an inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by Business Associate or Covered Entity to another similarly situated individual at the same facility, provided that any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed by any person.

*QHRC complies with all HIPAA regulations. If your organization has a standard BAA, we are willing to consider that agreement in lieu of this one.

b) *“Designated Record Set”* means a group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

For purposes of this definition, the term “record” means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

c) *“Electronic Protected Health Information”* or *“Electronic PHI”* means Protected Health Information that is transmitted by or maintained in electronic media as defined in the HIPAA Regulations.

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

e) *“HIPAA Regulations”* means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164, as in effect or as amended from time to time.

f) *“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.

g) *“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.

h) *“Unsecured Protected Health Information”* means PHI that is not rendered

unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

2) Obligations and Activities of Business Associate

a) *Use or Disclosure.* Business Associate agrees not to use or further disclose PHI created or received by Business Associate from or on behalf of Covered Entity other than as expressly permitted or required by this Agreement, as required by law, or as otherwise authorized in writing by the Covered Entity.

b) *Safeguards.* Business Associate agrees to use appropriate safeguards, consistent with applicable law, to prevent the access, use or disclosure of PHI other than as provided for by this Agreement. To the extent that Business Associate creates, receives, maintains or transmits Electronic PHI, Business Associate agrees to use appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of Covered Entity's Electronic PHI in accordance with the HIPAA Regulations.

c) *Mitigation.* Business Associate agrees to mitigate, to the extent practicable, any harmful effect caused by a use or disclosure of PHI by Business Associate in violation of this Agreement of which Business Associate becomes aware.

d) *Reporting.* Business Associate agrees to notify Covered Entity if Business Associate has knowledge that PHI has been used or disclosed by Business Associate in a manner that violates this Agreement as set forth in this paragraph. To the extent that Business Associate creates, receives, maintains or transmits Electronic PHI, Business Associate agrees to report promptly to Covered Entity any Security Incident, as determined by Business Associate, involving PHI of which Business Associate becomes aware. Business Associate will, following the discovery of a Breach of Unsecured PHI, notify Covered Entity of such Breach without unreasonable delay and in no event later than three (3) calendar days after the discovery. Business Associate will provide written notification to:

[Client name here]

including (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during the Breach, (ii) a brief description of what happened with the date of the breach and date of discovery of the breach, (iii) a description of the types of Unsecured Protected Health Information

involved in the breach, (iv) a description of what is being done to investigate the breach, mitigate the effects of the breach and protect from further breaches, (v) a description of how Business Associate will prevent future breaches from occurring, (vi) any steps individuals should take to protect themselves from potential harm resulting from the breach, and (vii) a description of the sanctions imposed on any members of the workforce involved in the breach. A Breach will be treated as discovered as of the first day on which such Breach is known or reasonably should have been known by Business Associate.

e) *Subcontractors and Agents.* Business Associate agrees to ensure that any subcontractor or agent, to whom Business Associate provides PHI received from, or created or received by Business Associate on behalf of the Covered Entity, agrees to comply with the restrictions, terms and conditions that apply through this Agreement to Business Associate with respect to such information.

f) *Access.* Upon request by Covered Entity for access to PHI about an individual contained in a Designated Record Set, Business Associate will make available to Covered Entity, in the time and manner reasonably designated by Covered Entity, such PHI for so long as such information is maintained in the Designated Record Set. In the event any individual requests access to PHI directly from Business Associate, Business Associate will forward such request to Covered Entity in the time and manner reasonably designated by the parties such that Covered Entity can respond to such individual in accordance with 45 C.F.R. § 164.524. Any denials of access to the PHI requested will be the responsibility of Covered Entity.

g) *Amendment.* Upon receipt of a written request by or on behalf of Covered Entity for the amendment of an individual's PHI or record contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), Business Associate will provide such information to Covered Entity for amendment, in the time and manner reasonably designated by the Covered Entity, and incorporate any such amendments in the PHI as required by 45 C.F.R. §164.526.

h) *Audit and Inspection.* Business Associate agrees to make its internal practices, books and records relating to the use and disclosure of PHI available to the Covered Entity and the Secretary of the United States Department of Health and Human Services and his/her designee (the "Secretary") for the purposes of determining Covered Entity's compliance with the Privacy Rule, in the time and manner designated by the Covered Entity or the Secretary.

i) *Documentation of Disclosure.* Business Associate agrees to comply with the requirements governing documentation of disclosures of PHI and any information related to such disclosures as are imposed upon Covered Entity under 45 C.F.R. § 164.528.

j) *Accounting.* Business Associate agrees to provide to Covered Entity or an Individual information compiled by Business Associate in accordance with Section 2.i. hereof, in the time and manner designated by the parties for a reasonable cost-based fee (under conditions permitted by HIPAA if an Individual requests an accounting more than once during a twelve month period).

k) *Compliance with the HITECH Standards.* Notwithstanding any other provision in this Agreement, no later than February 17, 2010, unless a separate effective date is specified by law or this Agreement for a particular requirement (in which case the separate effective date will be the effective date for that particular requirement), Business Associate will comply with the HITECH Standards, including, but not limited to: (i) compliance with the requirements regarding minimum necessary under HITECH § 13405(b); (ii) requests for restrictions on use or disclosure to health plans for payment or health care operations purposes when the provider has been paid out of pocket in full consistent with HITECH § 13405(a); (iii) the prohibition of sale of PHI without authorization unless an exception under HITECH § 13405(d) applies; (iv) the prohibition on receiving remuneration for certain communications that fall within the exceptions to the definition of marketing under 45 C.F.R. § 164.501 unless permitted by this Agreement and §13406 of HITECH; (v) the requirements relating to the provision of access to certain information in electronic access under HITECH § 13405(e); (vi) compliance with each of the Standards and Implementation Specifications of 45 C.F.R. §§ 164.308 (Administrative Safeguards), 164.310 (Physical Safeguards), 164.312 (Technical Safeguards) and 164.316 (Policies and Procedures and Documentation Requirements); and (vii) as of the separate compliance date set forth in regulations promulgated under HITECH on this topic, the requirements regarding accounting of certain disclosures of PHI maintained in an Electronic Health Record under HITECH § 13405(c).

l) *Standard Transactions.* If Business Associate conducts in whole or in part Standard Transactions, for or on behalf of Covered Entity, Business Associate will comply, and will require any subcontractor or agent involved with the conduct of such Standard Transactions to comply, with each applicable requirement of 45 CFR part 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that: (a) changes the definition, data

condition, or use of a data element or segment in a Standard Transaction; (b) adds any data elements or segments to the maximum defined data set; (c) uses any code or data element that is marked “not used” in the Standard Transaction’s implementation specification or is not in the Standard Transaction’s implementation specification; or (d) changes the meaning or intent of the Standard Transaction’s implementation specification.

m) *Security Rule.* The Business Associate shall: (a) 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; (b) ensure that any agent, including a subcontractor, to whom it provides such electronic protected health information agrees to implement reasonable and appropriate safeguards to protect the electronic protected health information; and report to the Covered Entity any security incident to which it becomes aware.

3) Permitted Uses and Disclosures by Business Associate

a) *General Use and Disclosure Provisions.* Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI in connection with its performance of the services under the Underlying Agreement if such use or disclosure of Protected Health Information would not violate HIPAA, the HIPAA Regulations or HITECH if done by Covered Entity or such use or disclosure is expressly permitted under Section 3.b. (“Specific Use and Disclosure Provisions”) of this Agreement.

b) *Specific Use and Disclosure Provisions.*

(i) Except as otherwise limited in this Agreement, Business Associate may use and disclose Protected Health Information for the proper management and administration of the Business Associate or to meet its legal responsibilities; provided, however, that such Protected Health Information may be disclosed for such purposes only if the disclosures are required by law or the Business Associate obtains the following reasonable assurances from the person to whom the information is disclosed:

(a) the information will remain confidential;

(b) the information will be used or further disclosed only as required by law or for the purpose for which the information was disclosed to the person; and

(c) the person will notify the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(ii) Business Associate may use and disclose Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

(iii) *Data Aggregation.* Business Associate may use and disclose PHI received by Business Associate in its capacity as a Business Associate of Covered Entity to provide Data Aggregation services relating to the health care operations of Covered Entity, provided that Business Associate notifies Covered Entity in advance of intended Data Aggregation services.

4) Obligations of Covered Entity

a) Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity or that is not otherwise expressly permitted under this Agreement.

b) Covered Entity will notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity 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.

c) Covered Entity will notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

d) Covered Entity will 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.

e) Covered Entity agrees that it will have entered into "Business Associate Agreements" with any third parties (e.g., case managers, brokers or third party administrators) to which Covered Entity directs and authorizes Business Associate to disclose PHI.

5) Term and Termination

a) *Term.* This Agreement will be effective as of the Effective Date and will continue unless or until this Agreement is terminated in accordance with the provisions of §§ 5.b. or 6.b. hereof or the Underlying Agreement is terminated.

b) *Termination for Cause.* Without limiting the termination rights of the parties pursuant to the Underlying Agreement,

(i) In the event of a material breach by Business Associate of its obligations hereunder, Covered Entity will notify Business Associate of such breach and Business Associate will have thirty (30) days to cure such breach. In the event Business Associate does not cure the breach, or cure is infeasible, Covered Entity will have the right to immediately terminate this Agreement and the Underlying Agreement. If cure of the material breach is infeasible, Covered Entity will report the violation to the Secretary.

(ii) As of February 17, 2010, upon Business Associate's knowledge of a material breach by Covered Entity of this Agreement, Business Associate will notify Covered Entity of such breach and Covered Entity will have thirty (30) days to cure such breach. In the event Covered Entity does not cure the breach, or cure is infeasible, Business Associate will have the right to immediately terminate this Agreement and the Underlying Agreement. If cure of the material breach is infeasible, Business Associate will report the violation to the Secretary.

c) *Effect of Termination.* Upon termination of the Underlying Agreement for any reason, Business Associate will return or destroy all PHI that Business Associate or its subcontractors or agents received from Covered Entity in any form and will not retain any copies of such PHI, provided, if Business Associate determines, in its sole discretion, that returning or destroying the PHI is not feasible, Business Associate will comply with the provisions of this Agreement applicable to the uses and disclosures of PHI for so long as Business Associate maintains such PHI.

6) Miscellaneous

a) *Regulatory References.* A reference in this Agreement to a section in HIPAA, the HIPAA Regulations or the HITECH Standards means the section as in effect or as amended from time to time, and for which compliance is required.

b) *Amendment.* Covered Entity and Business Associate agree that

amendment of this Agreement may be required to ensure that Covered Entity and Business Associate comply with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of Protected Health Information, including, but not limited to, changes under the HIPAA Regulations and the HITECH Standards. If the Covered Entity determines that this Agreement must be amended to comply with such laws and regulations, it shall provide Business Associate thirty days notice prior to the amendment's effective date. If the Business Associate disputes the amendment, it shall provide notice of such dispute to Covered Entity prior to the expiration of the thirty day notice period. Upon the receipt of such dispute from Business Associate, Business Associate and Covered Entity shall attempt to negotiate an alternate amendment within thirty days following such notice of dispute. If the parties fail to negotiate an alternative amendment at the end of the thirty days, the Agreement shall terminate.

c) *Survival.* The respective rights and obligations of Business Associate under Section 5.c. hereof will survive the termination of this Agreement.

d) *Interpretation.* Any ambiguity in this Agreement will be resolved in favor of a meaning that permits Covered Entity to comply with HIPAA, the HIPAA Regulations, the HITECH Standards and any other applicable law protecting the privacy, security and confidentiality of PHI. To the extent that any provisions of this Agreement conflict with the provisions of the Underlying Agreement or any other agreement or understanding between the parties, this Agreement will control.

e) *State Law.* Nothing in this Agreement will be construed to require Business Associate to use or disclose PHI in violation of New York State law.

f) *No Third Party Beneficiaries.* Nothing express or implied in this Agreement is intended or will be deemed to confer upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, obligations, remedies or liabilities.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Effective Date.

Qualitative Health Research Consultants, LLC

ORGANIZATION

Signature

Signature

Cameron L. Macdonald
Partner & Co-Founder

Name

Title