Business Associate Agreement

Quantitative Medical Systems, Inc., d/b/a Constellation Kidney Group ("***Business Associate***") and the entity that receives any Products from Business Associate under the Underlying Agreement (the "***Covered Entity***") enter into this Business Associate Agreement ("***BAA***"), which shall apply to the extent that (i) Business Associate receives PHI (as hereinafter defined) from Covered Entity, and (ii) either the Underlying Agreement expressly incorporates this BAA by reference or the parties sign this BAA.

This BAA is supplemental to, and forms an integral part of, the Underlying Agreement and is effective upon the earlier of signature or its incorporation into the Underlying Agreement, which incorporation may be specified in the Underlying Agreement or an executed amendment to the Underlying Agreement (the "**Effective Date**"). In case of any conflict or inconsistency between the terms of the Underlying Agreement and this BAA, this BAA shall take precedence over the terms of the Underlying Agreement to the extent of such conflict or inconsistency. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. PREAMBLE AND DEFINITIONS.

1.1 Definitions:

(a) "**Applicable Healthcare Law**" means any laws and regulations that apply to PHI exchanged under the Underlying Agreement, including HIPAA, HIPAA Rules, the HITECH Act, and the ARRA.

(b) "**Breach**" means the acquisition, access, use, or disclosure of Unsecured PHI (as hereinafter defined) in a manner not permitted under the Privacy Rule (as hereinafter defined) which compromises the security or privacy of the Unsecured PHI, excluding:

(i) Any unintentional acquisition, access, or use of Unsecured PHI by a workforce member or person acting under the authority of the Covered Entity the Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule;

(ii) Any inadvertent disclosure by a person who is authorized to access Unsecured PHI at the Covered Entity or Business Associate to another person authorized to access Unsecured PHI at the Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule;

(iii) A disclosure of Unsecured PHI where the Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; and

(iv) Instances where there is a low probability that the Unsecured PHI has been compromised based on a risk assessment which considers the factors identified in 45 C.F.R. § 164.402.

(c) "**Products**" means the goods and services provided by Business Associate to Covered Entity under the Underlying Agreement.

(d) "**Security Incident**" is as defined under 45 C.F.R. § 164.304, with the exception that Unsuccessful Security Incidents, as defined below, shall not be considered Security Incidents.

(e) "**Underlying Agreement**" means the written or electronic agreement which governs the provision of the Products.

(f) "**Unsecured PHI**" means PHI (as hereinafter defined) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

(g) "**Unsuccessful Security Incident**" means an attempted unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that does not actually result in unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

1.2 This BAA is intended to ensure that Business Associate will establish and implement appropriate safeguards for the Protected Health Information (**"PHI"**) (as defined under the HIPAA Rules) that Business Associate may receive, create, maintain, use, or disclose in connection with the functions, activities, and Products that Business Associate performs for Covered Entity. The functions, activities, and services that Business Associate performs for Covered Entity are defined in the Underlying Agreement. For the sake of clarity, this BAA shall not apply in the event that Business Associate does not receive, create, maintain, use, or disclose PHI in connection with the Underlying Agreement.

1.3 This BAA is entered into pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended (**"HIPAA"**). Pursuant to changes required under the Health Information Technology for Economic and Clinical Health Act of 2009 (the **"HITECH Act"**) and under the American Recovery and Reinvestment Act of 2009 (**"ARRA"**), this BAA also reflects federal breach notification requirements imposed on Business Associate when "Unsecured PHI" (as defined under the HIPAA Rules) is acquired by an unauthorized party, and the expanded privacy and security provisions imposed on business associates.

1.4 Unless the context clearly indicates otherwise, the following terms in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, disclosure, Electronic Media, Electronic Protected Health Information (ePHI), Health Care Operations, individual, Minimum Necessary, Notice of Privacy Practices, Required By Law, Secretary, Subcontractor, Unsecured PHI, and use.

1.5 A reference in this BAA to the Privacy Rule means the Privacy Rule, in conformity with the regulations at 45 C.F.R. Part 160 and Subparts A and E of Part 164 (the **"Privacy Rule"**) as interpreted under applicable regulations and guidance of general application published by HHS, including all amendments thereto for which compliance is required, as amended by ARRA and the HITECH Act. A reference in this BAA to the Security Rule means the Security Rule, as described in the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Part 160 and Subparts A and C of Part 164, as amended by ARRA and the HITECH Act (the "**Security Rule**"). The Privacy Rule and Security Rule are collectively referred to herein as the "**HIPAA Rules**." A reference in this BAA to a section in the HIPAA Rules means the section as in effect or as amended.

2. **GENERAL OBLIGATIONS OF BUSINESS ASSOCIATE**.

2.1 Business Associate agrees not to use or disclose PHI, other than as permitted or required by this BAA or as Required By Law, or if such use or disclosure does not otherwise cause a Breach of Unsecured PHI.

2.2 Business Associate agrees to use appropriate safeguards, and otherwise comply with the Privacy Rule and Security Rule, to protect and prevent the use or disclosure of PHI and Electronic Protected Health Information ("ePHI") other than as provided for by the BAA.

2.3 Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result of a use or disclosure of PHI by Business Associate in violation of this BAA's requirements or that would otherwise cause a Breach of Unsecured PHI.

2.4 The Business Associate agrees to the following Security Incident and Breach notification requirements:

(a) Business Associate agrees to report to Covered Entity any Security Incident of which it becomes aware within thirty (30) calendar days of "discovery" within the meaning of the HITECH Act, except that, with respect to any occurrences of Unsuccessful Security Incidents, this section shall hereby serve as notice, and no additional reporting shall be required to Covered Entity. Otherwise, a notice of a Security Incident shall include the identification of whether the Security Incident is also a Breach, the general nature of the Security Incident, whether the Security Incident is ongoing, and whether means through which the Security Incident occurred has been or is being addressed.

(b) Business Associate agrees to report to Covered Entity any Breach of which it becomes aware within thirty (30) calendar days of "discovery" within the meaning of the HITECH Act. Business Associate's notification of a Breach under this Section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA, the HIPAA Rules, and related guidance issued by the Secretary or the delegate of the Secretary from time to time. Specifically, a notice of a Breach shall include the following:

(i) To the extent possible, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the breach;

(ii) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(iii) A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(iv) Any steps individuals should take to protect themselves from potential harm resulting from the Breach;

(v) A brief description of what the covered entity involved is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further breaches; and

(vi) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(c) In the event Business Associate becomes aware of a Breach, Covered Entity hereby agrees that Business Associate may, in its discretion, provide any notices of Breach or Security Incident to applicable authorities and/or affected individuals that are required by any applicable state or federal law, provided that Covered Entity shall have the right to propose commercially reasonable edits to any such notices; otherwise, if Business Associate defers to Covered Entity to provide any such notices then Business Associate shall provide Covered Entity with such reasonable assistance as necessary to enable Covered Entity to provide any such notices. Covered Entity may, at its own effort and expense, send any notices that are not required by applicable law.

(d) In the event of a Breach or Security Incident for which Business Associate elects to send notices required by applicable state or federal law, Business Associate bears the burden of demonstrating that notices as required by applicable state or federal law were made, including evidence demonstrating the necessity of any delay, or that the unauthorized use or disclosure did not constitute a Breach or a Security Incident.

2.5 Business Associate agrees, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to require that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

2.6 Business Associate agrees to make available PHI in a Designated Record Set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.524 within twenty (20) days of receiving written request by Covered Entity.

(a) In the event Business Associate receives a request directly from an individual in regard to the individual exercising their rights under 45 C.F.R. § 164.524, Business Associate shall forward the request to the Covered Entity within twenty (20) days of receipt of the request.

(b) Business Associate agrees to comply with a Covered Entity’s request to restrict the disclosure of an individual’s PHI in a manner consistent with 45 C.F.R. § 164.522, except where such use, disclosure, or request is required or permitted under applicable law.

(c) To the extent Business Associate is permitted by Covered Entity to respond to requests Business Entity receives from individuals, Business Associate agrees to charge fees related to providing individuals access to their PHI in accordance with 45 C.F.R. § 164.524(c)(4).

(d) Business Associate agrees that when requesting, using, or disclosing PHI in accordance with 45 C.F.R. § 164.502(b)(1) that such request, use, or disclosure shall be to the minimum extent necessary, including the use of a "limited data set" as defined in 45 C.F.R. §

164.514(e)(2), to accomplish the intended purpose of such request, use, or disclosure, as interpreted under related guidance issued by the Secretary from time to time.

2.7 Business Associate agrees to make any amendments to PHI in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or to take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526.

2.8 Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.528.

2.9 In the event Business Associate receives a request directly from an individual in regard to the individual exercising their rights under 45 C.F.R. § 164.526 or 45 C.F.R. § 164.528, Business Associate shall forward the request to the Covered Entity within forty (40) days of receipt of the request.

2.10 Business Associate agrees to make its internal practices, books, and records, including policies and procedures regarding PHI, relating to the use and disclosure of PHI and Breach of any Unsecured PHI received from Covered Entity, or created or received by the Business Associate on behalf of Covered Entity, available to the Secretary for the purpose of the Secretary determining compliance with the Privacy Rule.

2.11 To the extent that Business Associate agrees to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s).

2.12 Business Associate agrees to account for the following disclosures:

(a) Business Associate agrees to maintain and document disclosures of PHI and Breaches and any information relating to the disclosure of PHI and Breach of Unsecured PHI in a manner as would be required under Applicable Healthcare Law for Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches.

(b) Business Associate agrees to provide to Covered Entity information collected in accordance with this Section 2.12, as required under Applicable Healthcare Law to permit Covered Entity to respond to a request by an individual or the Secretary for an accounting of PHI disclosures and Breaches of Unsecured PHI.

(c) Business Associate agrees to account for any disclosure of PHI used or maintained as an Electronic Health Record (as defined in Section 5) (**"EHR"**) in a manner consistent with 45 C.F.R. § 164.528 and related guidance issued by the Secretary from time to time; provided that, where required under Applicable Healthcare Law, an individual shall have the right to receive an accounting of disclosures of EHR by the Business Associate made on behalf of the Covered Entity only during the three years prior to the date on which the accounting is requested from Covered Entity.

(d) In the case of an EHR that the Business Associate acquired on behalf of the Covered Entity as of January 1, 2009, paragraph (c) above shall apply to disclosures with

respect to PHI made by the Business Associate from such EHR on or after January 1, 2014. In the case of an EHR that the Business Associate acquires on behalf of the Covered Entity after January 1, 2009, paragraph (c) above shall apply to disclosures with respect to PHI made by the Business Associate from such EHR on or after the later of January 1, 2011, or the date that it acquires the EHR.

2.13 Business Associate agrees to comply with the "Prohibition on Sale of Electronic Health Records or Protected Health Information," as provided in Section 13405(d) of Subtitle D (Privacy) of ARRA, and the "Conditions on Certain Contacts as Part of Health Care Operations," as provided in Section 13406 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.

2.14 Business Associate acknowledges that, effective on the Effective Date of this BAA, it may be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. § 1320d-5 and 1320d-6, as amended, for failure to comply with any of the use and disclosure requirements of this BAA and any guidance issued by the Secretary from time to time with respect to such use and disclosure requirements.

3. **PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**.

3.1 General Uses and Disclosures. Business Associate agrees to receive, create, use, or disclose PHI only in a manner that is consistent with this BAA, the Privacy Rule, or Security Rule, and only in connection with providing services to Covered Entity; provided that the use or disclosure would not violate the Privacy Rule, including 45 C.F.R. § 164.504(e), if the use or disclosure would be done by Covered Entity. For example, the use and disclosure of PHI will be permitted for "treatment, payment, and health care operations," in accordance with the Privacy Rule.

3.2 Business Associate may use or disclose PHI as Required By Law.

3.3 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.

3.4 Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

3.5 Specific Other Uses and Disclosures:

(a) Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Business

Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Business Associate may provide data aggregation services relating to the health care operations of the Covered Entity.

4. **OBLIGATIONS OF COVERED ENTITY**.

4.1 Covered Entity shall:

(a) Provide Business Associate with the Notice of Privacy Practices that Covered Entity produces in accordance with the Privacy Rule, and any changes or limitations to such notice under 45 C.F.R. § 164.520, to the extent that such changes or limitations may affect Business Associate's use or disclosure of PHI.

(b) Notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to comply with under 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI under this BAA.

(c) Notify Business Associate of any changes in or revocation of permission by an individual to use or disclose PHI, if such change or revocation may affect Business Associate's permitted or required uses and disclosures of PHI under this BAA.

4.2 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 Applicable Healthcare Law if done by Covered Entity, except as provided under Section 3 of this BAA.

5. **COMPLIANCE WITH SECURITY RULE**.

5.1 Business Associate shall comply with the HIPAA Security Rule. The term **"Electronic Health Record"** or **"EHR"** as used in this BAA shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

5.2 In accordance with the Security Rule, Business Associate agrees to:

(a) Implement the administrative safeguards set forth at 45 C.F.R. § 164.308, the physical safeguards set forth at 45 C.F.R. § 164.310, the technical safeguards set forth at 45 C.F.R. § 164.312, and the policies and procedures set forth at 45 C.F.R. § 164.316, to reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Security Rule. Business Associate acknowledges that, effective on the Effective Date of this BAA, (a) the foregoing safeguards, policies, and procedures requirements shall apply to Business Associate in the same manner that such requirements apply to Covered Entity, and (b) Business Associate shall be liable under the civil and criminal enforcement provisions set forth at 42 U.S.C. § 1320d-5 and 1320d-6, as amended from time to time, for failure to comply with the safeguards, policies, and procedures requirements and any guidance issued by the Secretary from time to time with respect to such requirements;

(b) Require that any agent, including a Subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect the PHI; and

(c) Report to the Covered Entity any Security Incident of which it becomes aware in accordance with Section 2.4(a) of this BAA.

6. **INDEMNIFICATION**.

The parties agree and acknowledge that except as set forth herein, the indemnification obligations contained under the Underlying Agreement shall govern each party's performance under this BAA.

7. **TERM AND TERMINATION**.

7.1 This BAA shall be in effect as of the Effective Date, and shall terminate on the earlier of the date that:

(a) Either party terminates for cause as authorized under Section 7.2.

(b) All of the PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity. If the parties agree that it is not feasible to return or destroy PHI, protections are extended in accordance with Section 7.3.

7.2 Upon either party's knowledge of material breach by the other party, the non-breaching party shall provide an opportunity for the breaching party to cure the breach or end the violation. If the breaching party does not cure the breach or end the violation within a reasonable timeframe not to exceed thirty (30) days from the notification of the breach, the non-breaching party may terminate this BAA upon written notice to the other party. The termination of this BAA shall not affect the Underlying Agreement, except to the extent that a breach under this BAA otherwise entitles Covered Entity to terminate the Underlying Agreement per the terms of the Underlying Agreement.

7.3 Upon termination of this BAA for any reason, the parties agree that, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

(a) Retain only that PHI that is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities.

(b) Return to Covered Entity or, if agreed to by the parties, destroy the remaining PHI that the Business Associate still maintains in any form, except for that PHI that Business Associate is otherwise permitted to keep by applicable state or federal law.

(c) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to ePHI to prevent use or disclosure of the PHI, other than as provided for in this Section 7, for as long as Business Associate retains the PHI.

(d) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out in this BAA which applied prior to termination.

(e) Return to Covered Entity or, if agreed to by the parties, destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

7.4 The obligations of Business Associate under this Section 7 shall survive the termination of this BAA.

8. **MISCELLANEOUS**.

8.1 The parties agree to take such action as is necessary to amend this BAA to comply with the requirements of the Privacy Rule, the Security Rule, HIPAA, ARRA, the HITECH Act, the Consolidated Appropriations Act, 2021 (CAA-21), the HIPAA Rules, and any other applicable law.

8.2 The respective rights and obligations of Business Associate under Section 6 and Section 7 of this BAA shall survive the termination of this BAA.

8.3 This BAA shall be interpreted in the following manner:

(a) Any ambiguity shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Rules.

(b) Any inconsistency between the BAA's provisions and the HIPAA Rules, including all amendments, as interpreted by the HHS, a court, or another regulatory agency with authority over the Parties, shall be interpreted according to the interpretation of the HHS, the court, or the regulatory agency.

(c) Any provision of this BAA that differs from those required by the HIPAA Rules, but is nonetheless permitted by the HIPAA Rules, shall be adhered to as stated in this BAA.

8.4 This BAA constitutes the entire agreement between the parties related to the subject matter of this BAA, except to the extent that the Underlying Agreement imposes more stringent requirements related to the use and protection of PHI upon Business Associate. This BAA supersedes all prior negotiations, discussions, representations, or proposals, whether oral or written. This BAA may not be modified in a manner that results in a material degradation of Covered Entity's duties and obligations under this BAA, unless done so in writing and signed by a duly authorized representative of both parties. If any provision of this BAA, or part thereof, is found to be invalid, the remaining provisions shall remain in effect.

8.5 Neither party may assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under this BAA, in each case whether voluntarily, involuntarily, by operations of law, or otherwise, without the prior written consent of the other party, except Business Associate may assign or otherwise transfer any of its rights, or delegate or otherwise transfer any of its obligations or performance, under the BAA to any of its affiliates without consent of Covered Entity, provided that the BAA will bind and inure to the benefit of any Business Associate successor or assignee.

8.6 This BAA may be executed in two or more counterparts, each of which shall be deemed an original.

8.7 Except to the extent preempted by federal law, this BAA shall be governed by and construed in accordance with the same internal laws as that of the Underlying Agreement. The courts that have jurisdiction over any disputes that arise under this BAA shall align with the courts identified in the Underlying Agreement.