

**[AMENDED AND RESTATED] BUSINESS ASSOCIATE AGREEMENT**

This [Amended and Restated] Business Associate Agreement (the “Agreement”) is made effective the \_\_\_ day of \_\_\_\_\_, 20\_\_\_, by and between \_\_\_\_\_, hereinafter referred to as “Covered Entity,” and EMS Management & Consultants, Inc., hereinafter referred to as “Business Associate” (individually, a “Party” and collectively, the “Parties”).

WITNESSETH:

WHEREAS, the Parties wish to enter into a Business Associate Agreement to ensure compliance with the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA Privacy and Security Rules”) (45 C.F.R. Parts 160 and 164) and the “Red Flag Rules” as found at 16 C.F.R. § 681.1 and applicable to creditors subject to the administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. § 1681s(a)(1); and

WHEREAS, the Health Information Technology for Economic and Clinical Health (“HITECH”) Act of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, modified the HIPAA Privacy and Security Rules (hereinafter, all references to the “HIPAA Privacy and Security Rules” include all amendments thereto set forth in the HITECH Act and any accompanying regulations); and

WHEREAS, the Parties have entered into a written or oral arrangement or arrangements (the “Agreements”) whereby Business Associate will provide certain services to Covered Entity and, pursuant to such Agreements, Business Associate may be considered a “business associate” of Covered Entity as defined in the HIPAA Privacy and Security Rules; and

WHEREAS, Business Associate may have access to Protected Health Information or Electronic Protected Health Information (as defined below) in fulfilling its responsibilities under the Agreements; [and

WHEREAS, prior to enactment of the HITECH Act, Covered Entity and Business Associate previously entered into a Business Associate Agreement and now intend this Agreement to supersede the prior agreement in order to comply with the requirements of the HITECH Act;] and

WHEREAS, Covered Entity wishes to comply with the HIPAA Privacy and Security Rules, and Business Associate wishes to honor its obligations as a Business Associate to Covered Entity; and

WHEREAS, in the event that Business Associate is engaged to perform any activity in connection with any “covered account” of Covered Entity as defined in 16 C.F.R. § 681.1 (commonly referred to as the “Red Flag Rules” and applicable to any “creditor” or any “service provider” providing any service to such creditor with regard to a covered account), Business Associate agrees to fully adopt and comply with the Red Flag Rules as are currently in effect and as may be promulgated in the future, including but not limited to the adoption of a Red Flag program that is compliant with applicable federal regulations, and to take all necessary and appropriate steps to ensure that its activities are conducted in accordance with the Red Flag Rules designed to detect, prevent and mitigate the risk of identity theft.

THEREFORE, in consideration of the Parties’ continuing obligations under the Agreements, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the provisions of this Agreement.

## I. DEFINITIONS

Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Privacy and Security Rules. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Privacy and Security Rules, as amended, or the Red Flag Rules, the HIPAA Privacy and Security Rules and the Red Flag Rules in effect at the time shall control. Where provisions of this Agreement are different than those mandated by the HIPAA Privacy and Security Rules or the Red Flag Rules, but are nonetheless permitted by the HIPAA Privacy and Security Rules or the Red Flag Rules, the provisions of this Agreement shall control.

The term “Breach” means the unauthorized acquisition, access, use, or disclosure of protected health information which 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. The term “Breach” does **not** include: (1) any unintentional acquisition, access, or use of protected health information by any employee or individual acting under the authority of a covered entity or business associate if (a) 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, respectively, with the covered entity or business associate, and (b) such information is not further acquired, accessed, used, or disclosed by any person; or (2) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and (3) any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

The term “Electronic Health Record” means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

The term “HIPAA Privacy and Security Rules” refers to 45 C.F.R. Parts 160 and 164 as currently in effect or hereafter amended.

The term “Protected Health Information” means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is reasonable basis to believe the information can be used to identify the individual. “Protected Health Information” includes, without limitation, “Electronic Protected Health Information,” as defined below.

The term “Electronic Protected Health Information” means Protected Health Information which is transmitted by or maintained in Electronic Media (as now or hereafter defined in the HIPAA Privacy and Security Rules).

The term “Red Flag Rules” refers to the provisions found at 16 C.F.R. § 681.1 as applicable to financial institutions and creditors subject to the administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. § 1681s(a)(1).

The term “Red Flag” has the same meaning as provided within 16 C.F.R. § 681.1(b)(9) and means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

The term “Secretary” means the Secretary of the Department of Health and Human Services.

The term “Unsecured Protected Health Information” means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance published in the Federal Register at 74 Fed. Reg. 19006 on April 27, 2009 and in annual guidance published thereafter.

## II. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

a. Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreements, provided that such use or disclosure would not violate the HIPAA Privacy and Security Rules if done by Covered Entity. Until such time as the Secretary issues regulations pursuant to the HITECH Act specifying what constitutes “minimum necessary” for purposes of the HIPAA Privacy and Security Rules, Business Associate shall, to the extent practicable, disclose only Protected Health Information that is contained in a limited data set (as defined in Section 164.514(e)(2) of the HIPAA Privacy and Security Rules), unless the person or entity to whom Business Associate is making the disclosure requires certain direct identifiers in order to accomplish the intended purpose of the disclosure, in which event Business Associate may disclose only the minimum necessary amount of Protected Health Information to accomplish the intended purpose of the disclosure.

b. Business Associate may use Protected Health Information in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate, provided that such uses are permitted under state and federal confidentiality laws.

c. Business Associate may disclose Protected Health Information in its possession to third parties for the purposes of its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that:

1. the disclosures are required by law; or

2. Business Associate obtains reasonable assurances from the third parties to whom the Protected Health Information is disclosed that the information will remain confidential and be used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party, and that such third parties will notify Business Associate of any instances of which they are aware in which the confidentiality of the information has been breached.

d. Until such time as the Secretary issues regulations pursuant to the HITECH Act specifying what constitutes “minimum necessary” for purposes of the HIPAA Privacy and Security Rules, Business Associate shall, to the extent practicable, access, use, and request only Protected Health Information that is contained in a limited data set (as defined in Section 164.514(e)(2) of the HIPAA Privacy and Security Rules), unless Business Associate requires certain direct identifiers in order to accomplish the intended purpose of the access, use, or request, in which event Business Associate may access, use, or request only the minimum necessary amount of Protected Health Information to accomplish the intended purpose of the access, use, or request. Covered Entity shall determine what quantum of information constitutes the “minimum necessary” amount for Business Associate to accomplish its intended purposes.

## III. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. Business Associate acknowledges and agrees that all Protected Health Information that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display by Covered Entity or its operating

units to Business Associate or is created or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

b. Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.

c. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement. Specifically, Business Associate will:

1. implement the administrative, physical, and technical safeguards set forth in Sections 164.308, 164.310, and 164.312 of the HIPAA Privacy and Security Rules that reasonably and appropriately protect the confidentiality, integrity, and availability of any Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, and, in accordance with Section 164.316 of the HIPAA Privacy and Security Rules, implement and maintain reasonable and appropriate policies and procedures to enable it to comply with the requirements outlined in Sections 164.308, 164.310, and 164.312; and

2. report to Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement of which Business Associate becomes aware. Business Associate shall report to Covered Entity any Security Incident of which it becomes aware. For purposes of this Agreement, "Security Incident" means the successful unauthorized access, use, disclosure, modification, or destruction of Protected Health Information or interference with system operations in an information system, of which Business Associate has knowledge or should, with the exercise of reasonable diligence, have knowledge, excluding (i) "pings" on an information system firewall; (ii) port scans; (iii) attempts to log on to an information system or enter a database with an invalid password or user name; (iv) denial-of-service attacks that do not result in a server being taken offline; or (v) malware (e.g., a worms or a virus) that does not result in unauthorized access, use, disclosure, modification or destruction of Protected Health Information.

d. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

e. Business Associate agrees to comply with any requests for restrictions on certain disclosures of Protected Health Information to which Covered Entity has agreed in accordance with Section 164.522 of the HIPAA Privacy and Security Rules and of which Business Associate has been notified by Covered Entity. In addition, and notwithstanding the provisions of Section 164.522 (a)(1)(ii), Business Associate agrees to comply with an individual's request to restrict disclosure of Protected Health Information to a health plan for purposes of carrying out payment or health care operations if the Protected Health Information pertains solely to a health care item or service for which Covered Entity has been paid by in full by the individual or the individual's representative.

f. At the request of Covered Entity and in a reasonable time and manner, Business Associate agrees to make available Protected Health Information required for Covered Entity to respond to an individual's request for access to his or her Protected Health Information in accordance with Section 164.524 of the HIPAA Privacy and Security Rules. If Business Associate maintains Protected Health Information electronically, it agrees to make such Protected Health Information available electronically to

the applicable individual or to a person or entity specifically designated by such individual, upon such individual's request.

g. At the request of Covered Entity and in a reasonable time and manner, Business Associate agrees to make available Protected Health Information required for amendment by Covered Entity in accordance with the requirements of Section 164.526 of the HIPAA Privacy and Security Rules.

h. Business Associate agrees to document any disclosures of and make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Privacy and Security Rules.

i. Business Associate agrees that it will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Secretary for the purpose of determining Covered Entity's compliance with the HIPAA Privacy and Security Rules, in a time and manner designated by the Secretary.

j. Business Associate agrees that, while present at any Covered Entity facility and/or when accessing Covered Entity's computer network(s), it and all of its employees, agents, representatives and subcontractors will at all times comply with any network access and other security practices, procedures and/or policies established by Covered Entity including, without limitation, those established pursuant to the HIPAA Privacy and Security Rules and the Red Flag Rules.

k. Business Associate agrees that it will not directly or indirectly receive remuneration in exchange for any Protected Health Information of an individual without the written authorization of the individual or the individual's representative, except where the purpose of the exchange is:

1. for public health activities as described in Section 164.512(b) of the Privacy and Security Rules;
2. for research as described in Sections 164.501 and 164.512(i) of the Privacy and Security Rules, and the price charged reflects the costs of preparation and transmittal of the data for such purpose;
3. for treatment of the individual, subject to any further regulation promulgated by the Secretary to prevent inappropriate access, use, or disclosure of Protected Health Information;
4. for the sale, transfer, merger, or consolidation of all or part of Business Associate and due diligence related to that activity;
5. for an activity that Business Associate undertakes on behalf of and at the specific request of Covered Entity;
6. to provide an individual with a copy of the individual's Protected Health Information pursuant to Section 164.524 of the Privacy and Security Rules; or
7. other exchanges that the Secretary determines in regulations to be similarly necessary and appropriate as those described in this Section III.k.

1. Business Associate agrees that it will not directly or indirectly receive remuneration for any written communication that encourages an individual to purchase or use a product or service without

first obtaining the written authorization of the individual or the individual's representative, unless:

1. such payment is for a communication regarding a drug or biologic currently prescribed for the individual and is reasonable in amount (as defined by the Secretary); or

2. the communication is made on behalf of Covered Entity and is consistent with the terms of this Agreement.

m. Business Associate agrees that if it uses or discloses patients' Protected Health Information for marketing purposes, it will obtain such patients' authorization before making any such use or disclosure.

#### IV. BUSINESS ASSOCIATE'S MITIGATION AND BREACH NOTIFICATION OBLIGATIONS

a. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

b. Following the discovery of a Breach of Unsecured Protected Health Information, Business Associate shall notify Covered Entity of such Breach without unreasonable delay and in no case later than forty-five (45) calendar days after discovery of the Breach. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to Business Associate or, through the exercise of reasonable diligence, would have been known to Business Associate.

c. Notwithstanding the provisions of Section IV.b., above, if a law enforcement official states to Business Associate that notification of a Breach would impede a criminal investigation or cause damage to national security, then:

1. if the statement is in writing and specifies the time for which a delay is required, Business Associate shall delay such notification for the time period specified by the official; or

2. if the statement is made orally, Business Associate shall document the statement, including the identity of the official making it, and delay such notification for no longer than thirty (30) days from the date of the oral statement unless the official submits a written statement during that time.

Following the period of time specified by the official, Business Associate shall promptly deliver a copy of the official's statement to Covered Entity.

d. The Breach notification provided shall include, to the extent possible:

1. the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during the Breach;

2. a brief description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

3. a description of the types of Unsecured Protected Health Information 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;

4. any steps individuals should take to protect themselves from potential harm resulting from the Breach;

5. a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and

6. 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.

e. Business Associate shall provide the information specified in Section IV.d., above, to Covered Entity at the time of the Breach notification if possible or promptly thereafter as information becomes available. Business Associate shall not delay notification to Covered Entity that a Breach has occurred in order to collect the information described in Section IV.d. and shall provide such information to Covered Entity even if the information becomes available after the forty-five (45)-day period provided for initial Breach notification.

#### V. WARRANTIES OF BUSINESS ASSOCIATE

Business Associate warrants:

a. That its internal practices, policies, and records relating to the use and disclosure of Protected Health Information will comply with the HIPAA Privacy and Security Rules; and

b. That it will train all of its employees, agents, representatives, and subcontractors on the network access and other security practices, procedures and/or policies established by Covered Entity including, without limitation, those established pursuant to the HIPAA Privacy and Security Rules and the Red Flag Rules prior to permitting such employees, agents, representatives, and subcontractors to be present at any Covered Entity facility and/or to access Covered Entity's computer network(s).

#### VI. OBLIGATIONS OF COVERED ENTITY

a. Upon request of Business Associate, Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with Section 164.520 of the HIPAA Privacy and Security Rules.

b. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information to which Covered Entity has agreed in accordance with Section 164.522 of the HIPAA Privacy and Security Rules, and Covered Entity shall inform Business Associate of the termination of any such restriction, and the effect that such termination shall have, if any, upon Business Associate's use and disclosure of such Protected Health Information.

#### VII. REQUIRED COMPLIANCE WITH RED FLAG RULES

In the event that Business Associate is engaged to perform an activity in connection with any

“covered account” as defined in 16 C.F.R. § 681.1 (as applicable to Covered Entity as a “creditor” and therefore to Business Associate as a “service provider” providing any service to Covered Entity), Business Associate agrees to: (i) fully adopt and comply with the Red Flag Rules currently in effect and as may be promulgated in the future; (ii) adopt a Red Flag program that is compliant with federal regulations as promulgated in 16 C.F.R. § 681.1; and (iii) take all necessary and appropriate steps to ensure that its activities undertaken as a part of this Agreement are conducted in accordance with the Red Flag Rules and its Red Flag program, including, without limitation, ensuring the adoption of and continued compliance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft, detecting any Red Flag that may arise during the term of this Agreement, reporting any such Red Flag to Covered Entity, and taking any such further steps as may be necessary to prevent or mitigate identity theft.

## VIII. TERM AND TERMINATION

a. Term. The Term of this Agreement shall be effective as of the date first written above, and shall terminate upon the later of the following events: (i) in accordance with Section VIII.c., when all of the Protected Health Information provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity or, if such return or destruction is infeasible, when protections are extended to such information; or (ii) upon the expiration or termination of the last of the Agreements.

b. Termination for Cause. Upon Covered Entity’s knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall have the right to immediately terminate this Agreement and the Agreements. If termination is not feasible, Covered Entity shall report such violation to the Secretary.

c. Effect of Termination.

1. Except as provided in paragraph 2. of this subsection, upon termination of this Agreement, the Agreements or upon request of Covered Entity, whichever occurs first, Business Associate shall within ten (10) days return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Neither Business Associate nor its subcontractors or agents shall retain copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide within ten (10) days to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

## IX. MISCELLANEOUS

a. Indemnification. Business Associate shall indemnify and hold Covered Entity harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards, or other expenses, of any kind or nature whatsoever, including, without limitations, attorneys’ fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or

alleged breach of this Agreement, or any Breach, by Business Associate or subcontractors or agents of Business Associate.

b. No Rights in Third Parties. Except as expressly stated herein, in the HIPAA Privacy and Security Rules, or in the Red Flag Rules, the Parties to this Agreement do not intend to create any rights in any third parties.

c. Survival. The obligations of Business Associate under Section VIII(c) of this Agreement shall survive the expiration, termination, or cancellation of this Agreement, the Agreements, and/or the business relationship of the parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

d. Amendment. This Agreement may be amended or modified only in a writing signed by the Parties. The Parties agree that they will negotiate amendments to this Agreement to conform to any changes in the HIPAA Privacy and Security Rules or Red Flag Rules as are necessary for Covered Entity to comply with the current requirements of the HIPAA Privacy and Security Rules, the Health Insurance Portability and Accountability Act, and the Red Flag Rules. In addition, in the event that either Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Privacy and Security Rules or any other applicable legislation including, but not limited to, the Red Flag Rules, then such Party shall notify the other Party of its belief in writing. For a period of up to thirty (30) days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty (30)-day period, the Agreement fails to comply with the HIPAA Privacy and Security Rules, the Red Flag Rules or any other applicable legislation, then either Party has the right to terminate this Agreement and the underlying arrangement upon written notice to the other party.

e. Assignment. Neither Party may assign its respective rights and obligations under this Agreement without the prior written consent of the other Party.

f. Independent Contractor. None of the provisions of this Agreement are intended to create, nor will they be deemed to create, any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other agreements between the Parties evidencing their business relationship.

g. Governing Law. To the extent this Agreement is not governed exclusively by the HIPAA Privacy and Security Rules, the Red Flag Rules, or other provisions of federal statutory or regulatory law, it will be governed by and construed in accordance with the laws of the state in which Covered Entity has its principal place of business.

h. No Waiver. No change, waiver, or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion.

i. Interpretation. Any ambiguity of this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the HIPAA Privacy and Security Rules and the Red Flag Rules.

j. Severability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect.

k. Notice. Any notification required in this Agreement shall be made in writing to the representative of the other Party who signed this Agreement or the person currently serving in that representative's position with the other Party.

l. Certain Provisions Not Effective in Certain Circumstances. The provisions of this Agreement relating to the HIPAA Security Rule shall not apply to Business Associate if Business Associate does not receive any Electronic Protected Health Information from or on behalf of Covered Entity.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

**Covered Entity:**

**Business Associate:**

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_