BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made this       day of      , 20     , by and between (“Covered Entity”) and  ("Business Associate") (collectively, the “Parties”).

**RECITALS**

WHEREAS, the Parties have entered into the **Agreement** dated       (the "Services Agreement") under which Business Associate will provide certain services to Covered Entity that will require Business Associate to have the use, receipt, or access to Covered Entity’s Protected Health Information (the “Services”) to perform the Services; and

WHEREAS, Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (“HIPAA”), and the implementing regulations promulgated thereunder from time to time by the U.S. Department of Health and Human Services (“HHS”), including but not limited to the Privacy, Security, Breach Notification and Enforcement Rules set forth in 45 C.F.R. Parts 160 and 164 (collectively, the “HIPAA Regulations”); and

WHEREAS, the HIPAA Regulations require Covered Entity to enter into a contract with Business Associate in order to provide for certain protections for the privacy and security of Protected Health Information, and to prohibit the disclosure to or use of Protected Health Information by Business Associate if such a contract is not in place; and

WHEREAS, the Parties desire to enter into this Agreement to govern the terms and conditions under which Business Associate may use, receive or access Covered Entity’s Protected Health Information to provide the Services, in accordance with HIPAA and the HIPAA Regulations.

NOW, THEREFORE, in consideration of the foregoing, each intending to be legally bound, the Parties agree as follows:

# **Section 1. Definitions**. The following terms used in this Agreement shall have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclose or Disclosure, Heath Care Operations, Individual, Minimum Necessary, Payment, Protected Health Information, Required by Law, Security Incident, Subcontractor, Treatment, Unsecured Protected Health Information, and Use.

### Specifically, Protected Health Information (“PHI”) means any information, whether oral or recorded in any form or medium, 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; identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes Electronic Protected Health Information (“ePHI”).

### Other terms used, but not otherwise defined in this Agreement shall have the same meanings as those terms in the HIPAA Regulations.

### **Section 2. Obligations of Business Associate.**

### 2.1Permitted Uses and Disclosures of Protected Health Information. Business Associate may use and disclose PHI received from and made available from Covered Entity or created by Business Associate on behalf of Covered Entity, only as necessary to perform the Services and as otherwise authorized by Covered Entity, provided that such use and disclosure would be permitted under state and federal confidentiality laws if done by Covered Entity, or as otherwise required by law or regulation. All other uses and disclosures not authorized by this Agreement are prohibited, without obtaining written authorization from Covered Entity. Notwithstanding the foregoing, Business Associate may use or disclose PHI for the specific uses and disclosures set forth below:

### Management and Administration. Business Associate may use and disclose PHI for the proper management and administration of Business Associate, or to carry out legal responsibilities of the Business Associate, provided that any disclosure is required by law, or Business Associate obtains reasonable assurances in writing from the person to whom the PHI is disclosed (i) that the PHI will remain confidential and will be used or further disclosed only for the purposes for which it was disclosed to the person; and (ii) the person is obligated to notify Business Associate (who will notify Covered Entity) of any instances of which it is aware in which the confidentiality of the PHI has been breached.

### Minimum Necessary. Business Associate may make uses and disclosures and requests for PHI consistent with 45C.F.R.164.502(b)(1). Business Associate agrees to use and disclose the minimum necessary PHI to accomplish tasks.

### 2.2 Security Rule Compliance. Business Associate shall establish, implement and maintain appropriate administrative, physical and technical safeguards in accordance with Subpart C of 45 C.F.R. Part 164 (the “Security Rule”) that reasonably and appropriately protect the confidentiality, integrity, and availability of any ePHI that it creates, receives, maintains, or transmits on behalf of Covered Entity and to prevent the use or disclosure of ePHI in any manner other than as permitted by this Agreement.

## 2.3 Mitigation. Business Associate agrees to mitigate, to the maximum extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

## 2.4 Reporting Non-Permitted Use and Disclosure of PHI and Breach Notification. Business Associate shall report to Covered Entity as soon as practicable and without unreasonable delay any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware. Business Associate shall make the initial report of the breach, including breaches of unsecured PHI and security incidents, immediately by e-mail to HIPAA@GenesisHCC.com followed by a written report to the Privacy Officer no later than forty-eight (48) hours from the date the Business Associate discovers the breach. The Business Associate report shall identify: (i) the nature of the non-permitted use or disclosure, (ii) the PHI used or disclosed, (iii) who made the non-permitted use or received the unauthorized disclosure and (v) what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure, and any other information necessary for Covered Entity to satisfy the provisions of HIPAA regulatory notification and reporting requirements.

## (a) For purposes of this Agreement and consistent with 45 C.F.R. § 164.402, a “breach” shall mean the acquisition, access, or use of PHI in a manner not permitted under the HIPAA Regulations (specifically, 45 C.F.R. Part 164, Subpart E) which compromises the security or privacy of the PHI. A breach shall be treated as discovered by Business Associate as of the first day on which such breach is known to the Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. Business Associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is an employee, officer, or other agent of Business Associate. Any impermissible use or disclosure of PHI by Business Associate is presumed to be a breach and shall be reported to Covered Entity, unless it can be demonstrated that there is a low probability that PHI has been compromised based upon a risk assessment that considers: (1) the nature and extent of the PHI involved in the breach; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to PHI has been mitigated. If the risk assessment evaluation fails to demonstrate there is a low probability that any PHI has been compromised, breach notification is required.

### In the event of a breach of PHI by Business Associate or any employee or agent of Business Associate, or a breach of PHI that is created, received, maintained, or transmitted by Business Associate on behalf of Covered Entity, Covered Entity shall provide the notices of breach that are required by 45 C.F.R. § 164. 404 and 45 C.F.R. § 164.406 to individuals and to the media, if media notice is required. Business Associate shall cooperate with Covered Entity in conducting the necessary risk assessment and providing information required for the notices. The notices must be provided without unreasonable delay, but in no case later than forty-five (45) days after Business Associate’s discovery of a breach. Business Associate shall make payment to Covered Entity to cover the costs of providing such notices necessitated by Business Associate’s breach prior to the time notices are to be mailed to individuals. Business Associate shall cover the costs of email and first class mail notices, any necessary substitute or alternative notices, media notices and the Covered Entity’s reasonable costs for investigation and management of the breach which will be charged to Business Associate on a pass-through basis. Failure to pay such amounts within said period will result in the addition of interest charges of 1.5% per month on any outstanding balance.

### 2.5 Use of Subcontractors and Agents. Business Associate shall ensure that any subcontractors or agents that create, receive, maintain or transmit PHI on behalf of Business Associate in connection with the Services it provides to Covered Entity under this Agreement shall agree to the same restrictions, conditions and requirements that apply to Business Associate with respect to such information, as provided in this Agreement, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), by requiring subcontractors and agents to enter into a written business associate agreement with Business Associate, incorporating such restrictions, conditions and requirements.

### 2.6 Availability of Internal Practices, Books and Records to Government Agencies. Business Associate shall make available to the Covered Entity, or to the Secretary of the U.S. Department of Health and Human Services ("Secretary"), its internal practices, books and records relating to the use and disclosure of PHI, in a time and manner designated by the Covered Entity or the Secretary, for purposes of determining compliance with HIPAA and the HIPAA Regulations.

### 2.7 Access by Individuals to PHI . Business Associate shall establish and maintain appropriate procedures to give individuals who are the subject of the PHI (or their designees, if applicable) access to their PHI in a designated record set held by Business Associate to satisfy Covered Entity’s obligations under 45 C.F.R. § 164.524.

### 2.8 Amendment of PHI. Business Associate shall make any amendment(s) 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 take other measures as necessary to satisfy Covered Entity’s obligations thereunder. Business Associate shall provide to Covered Entity such information as requested by Covered Entity to permit Covered Entity to respond to a request by an individual for an amendment to their PHI in accordance with the HIPAA Regulations within forty-five (45) days of receipt of a written request from Covered Entity.

### 2.9 Accounting of Disclosures. Upon Covered Entity's request, Business Associate shall provide to Covered Entity an accounting of all disclosures of PHI by Business Associate or its employees, agents, representatives or subcontractors, in accordance with the requirements of 45 C.F.R. § 164.528. At a minimum, within thirty (30) days of receipt of a written request from Covered Entity, Business Associate shall document and make available to Covered Entity or the individual, any information necessary to provide an accounting of disclosures in accordance with the requirements of the HIPAA Regulations. Business Associate shall maintain a process to provide this accounting of disclosures for as long as Business Associate maintains PHI received from or on behalf of Covered Entity. The accounting provided by Business Associate under this Section 2.9 shall include: the date of the disclosure; the name, and address if known, of the entity or person who received the PHI; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure. For each disclosure that requires an accounting under this Section 2.9, Business Associate shall track the information specified above, and shall securely maintain the information for six (6) years from the date of the disclosure.

### 2.10 Restrictions: Requests for Confidential Communications. Business Associate shall comply with any agreements for confidential communications of which it is aware and to which Covered Entity agrees pursuant to 45 C.F.R. §164.522(b) by communicating with individuals using agreed upon alternative means or alternative locations.

### 2.11 Compliance with Standard Transactions. Covered Entity is obligated to conduct Standard Transactions, as that term is defined in 45 C.F.R. § 162.103 in accordance with the requirements of 45 C.F.R. Part 162. If Business Associate conducts in whole or part Standard Transactions, for or on behalf of Company, 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 C.F.R. Part 162. Neither party will 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 Company that:

## (a) Changes the definition, data condition, or use of a data element or segment in a Standard Transaction;

## (b) Adds any data element or segment 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.

## 2.12 Acknowledgement of Application of Civil and Criminal Penalties. Business Associate acknowledges that under HIPAA, in the event that Business Associate does not comply with the requirements of the Agreement, criminal and civil penalties may be imposed by the Department of Health and Human Services in the same manner that such penalties apply to Covered Entity.

## **Section 3. Obligations of Covered Entity**

## 3.1 Notification of Changes to Notice of Privacy Practices. Covered Entity shall notify Business Associate of any changes in, or limitation(s) in the Notice of Privacy Practices that Covered Entity provides to individuals pursuant to the HIPAA Regulations, to the extent such limitation or change may affect Business Associate’s use or disclosure of PHI, by posting updates to the website at www.genesishcc.com.

# 3.2 Individual Revocation of Authorization. Covered Entity shall inform Business Associate of any changes in, or revocation of, the authorization provided to Covered Entity by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate’s use or disclosure of PHI under this Agreement.

# 3.3 Notification of Restrictions. Covered Entity shall notify Business Associate, in writing and in a timely manner, of any restrictions on 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 restrictions may affect Business Associate’s use or disclosure of PHI.

# 3.4 Permitted Use. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Regulations if done by Covered Entity.

# **Section 4. Term and Termination**

# 4.1 Term. The term of this Agreement shall be coterminous with the term of the Services Agreement.

# 4.2 Termination. In addition to and notwithstanding the termination provisions set forth in the Services Agreement, Covered Entity may terminate this Agreement immediately upon the provision of written notice to Business Associate if Business Associate has breached a material provision of this Agreement and Business Associate fails to cure the material breach within ten (10) days of receipt of written notice from Covered Entity regarding the existence of the material breach by Business Associate. Any breach related to the sale, transfer, or use or disclosure of PHI for commercial advantage, personal gain, or malicious harm shall be considered non-curable and shall be grounds for immediate termination. Business Associate's obligations under Article II and Section 4.3 shall survive the termination or expiration of this Agreement.

# 4.3 Disposition of PHI Upon Termination or Expiration. Upon termination or expiration of this Agreement for any reason, Business Associate shall, with respect to PHI received from Covered Entity, or created, maintained or received by Business Associate on behalf of Covered Entity, shall:

### Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

### Return to Covered Entity, or if agreed to by Covered Entity, destroy the remaining PHI that Business Associate still maintains in any form;

### Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. part 164 with respect to ePHI to prevent use of disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;

### 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 at Article II which applied prior to termination; and

### Return to Covered Entity (or if agreed to by Covered Entity, 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.

### The parties acknowledge and agree that if it is not feasible for Business Associate to return or destroy PHI, Business Associate must follow restrictions of this Section 4.3 regarding PHI retained, and must limit further uses and disclosures to those purposes that make return or destruction feasible.

### 4.4 Remedies Upon Breach of this Agreement or Covered Entity's Suspicion of Breach. Upon a breach or a suspected breach by Business Associate of any requirement of this Agreement, Covered Entity, at its option, may require Business Associate to:

### Furnish to Covered Entity copies of its practices and procedures and books and records to facilitate Covered Entity's mitigation of damages arising from an improper use or disclosure by Business Associate;

### Exercise all reasonable efforts to retrieve improperly used or disclosed PHI;

### Establish and adopt new practices, policies and procedures to assure that PHI is not used or disclosed in the future in violation of the HIPAA Privacy Standards;

### Comply with all auditing or reporting requests by Covered Entity to demonstrate Business Associate' compliance with the HIPAA Privacy Standards; and

### Take such other actions as Covered Entity may reasonably require, including termination of this Agreement.

### **Section 5. Miscellaneous**

## 5.1 No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement.

## 5.2 Indemnification. Business Associate agrees to indemnify, defend and hold harmless Covered Entity and Covered Entity’s employees, directors, officers, agents or other members of its workforce, each of the foregoing hereinafter referred to as "indemnified party," against all actual and direct losses suffered by an indemnified party and all liability to third parties arising from or in connection with any breach of this Agreement or of any warranty hereunder or from any negligence or wrongful acts or omissions, including failure to perform its obligations under the HIPAA Regulations, by Business Associate or its employees, directors, officers, subcontractors, agents or other members of its workforce. Accordingly, on demand, Business Associate shall reimburse any indemnified party for any and all actual and direct losses, liabilities, lost profits, fines, penalties, costs or expenses (including reasonable attorneys' fees) which may for any reason be imposed upon any indemnified party by reason of any suit, claim, action, proceeding or demand by any third party which results from Business Associate’s breach hereunder. Business Associate’s obligation to indemnify any indemnified party shall survive the expiration or termination of this Agreement for any reason.

## 5.3 Amendment to Comply with Law. The Parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that amendment of this Agreement may be required in future to provide for procedures to ensure compliance with such developments. The Parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations and other applicable laws relating to the security or confidentiality of PHI. The parties understand and agree that Covered Entity must receive satisfactory written assurance from Business Associate that Business Associate will adequately safeguard all PHI that it receives or creates pursuant to this Agreement. Upon Covered Entity's request, Business Associate agrees to promptly to enter into negotiations with Covered Entity concerning the terms of any amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA, the HIPAA Regulations or other applicable laws. Covered Entity may terminate this Agreement and Services Agreement upon thirty (30) days written notice in the event (i) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by Covered Entity pursuant to this Section or (ii) Business Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA and HIPAA Regulations.

## 5.4 Relationship to Services Agreement Provisions. In the event that a provision of this Agreement is contrary to a provision of the Services Agreement, the provision of this Agreement shall control. Otherwise, this Agreement shall be construed under, and in accordance with, the terms of the Services Agreement.

## 5.5 Severability. Any terms or provisions of this Agreement which will prove to be invalid, void or illegal will in no way affect, impair or invalidate any other term or provision herein and such remaining terms and provisions will remain in full force and effect.

## 5.6 Modification. This agreement may not be amended, modified, altered, or changed in any respect whatsoever except by a further agreement in writing, fully executed by each of the parties hereto.

## 5.7 Governing Law. This Agreement will be governed by and construed according to the laws of the state as provided in the Service Agreement.

## 5.8 Waiver of Breach. The waiver by either party of a breach or violation of any provision of this Agreement shall not operate as, or be construed to be, a waiver of any subsequent of the same or other provision hereof.

## 5.9 Relationship of the Parties. Business Associate and Covered Entity agree that their relationship under this Agreement shall be that of independent contracting parties and neither Covered Entity nor Business Associate shall be an agent, employee, partner or other legal representative of the other for any reason pursuant to this Agreement, or shall have the right to direct or control the performance of the other under this Agreement. The terms of this Agreement and the Services Agreement shall govern performance of the relationship.

## IN WITNESS WHEREOF, the parties hereto have executed this Agreement effective as of the date set forth above.

|  |  |
| --- | --- |
| COVERED ENTITY: | BUSINESS ASSOCIATE: |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | By: |
| Name: | Name: |
| Title: | Title: |