



**HIPAA BUSINESS ASSOCIATE AGREEMENT**

This HIPAA Business Associate Agreement ("Agreement") represents the agreement, including any prior or subsequent amendments or modifications thereto, between City of Glendale, the Covered Entity ("CE"), and Sterling Health Services, Inc., the Business Associate ("BA"), and is effective as of July 1, 2015.

**RECITALS**

- A. CE desires to disclose certain **Protected Health Information** ("PHI," defined below) including **Electronic Protected Health Information** ("EPHI," defined below) to BA pursuant to the terms of this Agreement.
- B. CE and BA acknowledge that in providing administration services for the Healthcare Flexible Spending Account (Healthcare FSA) and/or Health Reimbursement Arrangement (HRA) plan ("Plan") sponsored by CE, BA shall create, receive, modify, maintain and transmit, through electronic media and/or other means, PHI on behalf of CE. The scope and nature of the administration services that BA provides in connection with the Plan on behalf of CE are set forth in the Administration Services Agreement executed by the parties on July 1, 2015, and is incorporated herein by reference. Such services may include, inter alia, billing, adjudication, processing, and payment of healthcare claims, utilization review, data aggregation, and miscellaneous accounting and consulting services.
- C. CE and BA intend to protect the privacy and security of PHI in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), and all other applicable laws and regulations, including, but not limited to 45 CFR Parts 160 and 164.
- D. As defined under HIPAA, BA is required to enter into a contract with CE that details how BA will protect against the unauthorized use or disclosure of PHI.

The parties agree as follows:

**1. Definitions:** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the **Security and Privacy Rules**.

- a. **"Privacy Rule"** shall mean the HIPAA regulation that is codified at 45 CFR Parts 160 and 164, Subparts A, D, and E.
- b. **"Security Rule"** shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, Subpart C.
- c. **"Protected Health Information"** (PHI) shall have the same meaning as the term "protected health information," as defined in the **Security and Privacy Rules**, limited to the information created or received by BA from or on behalf of CE.

- d. **"Electronic Protected Health Information"** shall have the same meaning as the term "electronic protected health information," as defined in the **Security and Privacy Rules**, limited to the information created or received by BA from or on behalf of CE.
- e. **"Designated Record Set"** shall have the same meaning as the term "designated record set," as defined in the **Security and Privacy Rules**.
- f. **"Required By Law"** shall have the same meaning as the term "required by law," as defined in the **Security and Privacy Rules**.
- g. **"Secretary"** shall mean the Secretary of the Department of Health and Human Services.
- h. **"Security Incident"** shall have the same meaning as the term "security incident," as defined in the **Security and Privacy Rules**.
- i. **"Individual"** shall have the same meaning as the term "individual," as defined in the **Security and Privacy Rules**.
- j. **"Treatment"** shall have the same meaning as the term "treatment," as defined in the **Security and Privacy Rules**.
- k. **"Payment"** shall have the same meaning as the term "payment," as defined in the **Security and Privacy Rules**.
- l. **"Operations"** shall have the same meaning as the term "operations," as defined in the **Security and Privacy Rules**.
- m. **"Breach"** shall mean the acquisition, access, use, or disclosure of PHI in a manner that is not permitted by the **Security and Privacy Rules**.
- n. **"Privacy Officer"** shall mean the person designated by CE to serve as its privacy officer within the meaning of 45 CFR 164.530(a), and any person to whom the Privacy Officer has delegated any of his or her duties or responsibilities.
- o. **"Subcontractor"** shall have the same meaning given to it in 45 CFR 160.103
- p. **"HITECH Act"** shall mean the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act, Pub. L. No. 111-5.
- q. **"Unsecured Protected Health Information"** shall mean Protected Health Information in any form, including electronic, paper, or verbal, that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary pursuant to the HITECH Act, as such guidance may be updated by the Secretary from time to time.

## 2. **Obligations and Activities of BA:**

### **BA agrees:**

- a. not to use or further disclose PHI other than as permitted or required by this Agreement or as **Required by Law**;
- b. to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement;
- c. to mitigate, to the extent practicable, any harmful effect that is known to the BA of a use or disclosure of PHI by BA in violation of the requirements of this Agreement;
- d. to promptly report to the Privacy Officer of the CE any use or disclosure of PHI not provided by this agreement of which it becomes aware;

- e. to promptly report any Breaches of Unsecured Protected Health Information to the Privacy Officer of the CE. Such report must include at least the following information:
  - (1) The identity of each individual whose information was accessed, acquired, or disclosed during the breach;
  - (2) A brief description of what happened;
  - (3) The date of discovery of the breach;
  - (4) The nature of the Unsecured Protected Health Information that was involved (e.g. social security numbers, date of birth, etc.);
  - (5) Any steps individuals should take to protect themselves from potential harm resulting from the breach, and;
  - (6) A brief description of what the BA is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
- f. to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the CE, and, effective February 17, 2010, to comply with the provisions of the Security Rule identified in Section 3(a)(1)(B) of this Agreement;
- g. to ensure that any agent, including a subcontractor, to whom it provides EPHI agrees to implement reasonable and appropriate safeguards to protect it;
- h. to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by BA on behalf of CE agrees to the same restrictions and conditions that apply through this Agreement to BA with respect to such information;
- i. to provide access to PHI in a **Designated Record Set** to CE within ten days of a request of CE, in the time and manner designated by CE, or, as directed by CE, to an **Individual**, in order to meet the requirements of 45 CFR § 164.524;
- j. to make any amendment(s) to PHI in a **Designated Record Set** that the CE directs or to which the CE agrees pursuant to 45 CFR § 164.526, at the request of CE or an **Individual**, and in the time and manner designated by CE;
- k. to provide communications of Protected Health Information to an Individual by alternative means or at alternative locations, as directed by CE;
- l. to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by BA on behalf of CE, available to the CE, or, at request of the CE to the **Secretary**, in a time and manner designated by the CE or the **Secretary**, for the purposes of the **Secretary** determining CE's compliance with the **Privacy Rule**;
- m. to document such disclosures of PHI and information related to such disclosures as would be required for CE to respond to a request by **Individual** for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528;
- n. to provide to CE or an **Individual**, in a time and manner designated by CE, information collected in accordance with Section 2(l) of this Agreement, to permit CE to respond to a request by an **Individual** for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528;
- o. to report to CE as soon as practicable but in no event later than five (5) business days after discovery of any material attempted or successful unauthorized access, use, disclosure, loss, theft, modification, or destruction of PHI, or interference with system operations within an information system; and

- p. to the extent that BA provides services in connection with an account maintained by the CE that permits patients to make multiple payments for services rendered by the CE (including, but not limited to, billing and collection services), BA shall have and follow policies to detect and prevent identity theft in accordance with the identity theft regulations of the Federal Trade Commission, 16 C.F.R. § 681.2. In addition, in such case BA shall: (1) report to CE any pattern, practice, or specific activity that indicates the possible existence of identity theft ("Red Flags") involving anyone associated with CE, including its patients, employees, and contractors, and (2) take appropriate steps to prevent or mitigate identity theft when a Red Flag is detected.

### 3. Permitted Uses and Disclosures by BA:

#### a. Statutory Duties

- (1) BA acknowledges that it has a statutory duty under the HITECH Act to, among other duties:
  - (A) Effective February 17, 2010, use and disclose PHI only in compliance with 45 C.F.R. § 164.504(e)(the provisions of which have been incorporated into this Agreement); and
  - (B) Effective February 17, 2010, comply with 45 C.F.R §§ 164.308 ("Administrative Safeguards"), 164.310 ("Physical Safeguards"), 164.312 ("Technical Safeguards"), and 164.316 ("Policies and Procedures and Documentation Requirement"). In complying with 45 C.F.R. § 164.312 ("Technical Safeguards"), BA shall consider guidance issued by the Secretary pursuant to Section 13401(c) of the HITECH Act and, if a decision is made to not follow such guidance, document the rationale for that decision.
- (2) BA acknowledges that its failure to comply with these or any other statutory duties could result in civil and/or criminal penalties under 42 U.S.C §§ 1320d-5 and 1320d-6.

#### b. General Use and Disclosure Provisions

Except as otherwise limited in this Agreement, CE agrees that BA may use or disclose PHI on behalf of, or to provide services to, CE if such use or disclosure of PHI would not violate the **Security and Privacy Rules** if done by CE.

#### c. Specific Use and Disclosure Provisions

- (1) Except as otherwise limited in this Agreement, BA may use PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA;
- (2) Except as otherwise limited in this Agreement, BA may disclose PHI for the proper management and administration of the BA, provided that disclosures are **Required By Law**, or BA obtains reasonable assurance from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as **Required By Law** or for the purpose for which it was disclosed to the person, and the person notifies the BA of any instances of which it is aware in which the confidentiality of the information has been breached;
- (3) Except as otherwise limited in this Agreement, BA may use PHI to provide Data Aggregation services to CE as permitted by 45 CFR § 164.504(e)(2)(i)(B);
- (4) BA may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F. R. § 164.502(j)(1); and
- (5) As of the effective date of Section 13405(d) of the HITECH Act, BA may not receive direct or indirect remuneration in exchange for PHI unless permitted by the Act or regulations issued by the Secretary;

#### 4. **Obligations of CE:**

##### **CE shall:**

- a. notify affected Individuals, the Secretary, and, in certain circumstances, the media upon receiving notice from BA of a discovery of a breach of Unsecured PHI by BA, and shall do so within sixty (60) days following discovery of the breach pursuant to Section 6 (b).
- b. notify BA of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect BA's use or disclosure of PHI;
- c. provide BA with any changes in, or revocation of, permission by *Individual* to use or disclose PHI, if such changes affect BA's permitted or required uses and disclosures; and
- d. notify BA of any restriction to the use or disclosure of PHI that CE has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect BA's use or disclosure of PHI.

#### 5. **Permissible Requests by Covered Entity**

CE shall not request BA to use or disclose PHI in any manner that would not be permissible under the *Privacy Rule* if done by CE.

#### 6. **Notice of Breach of Unsecured PHI**

- a. BA Requirements. Pursuant to 45 CFR 164.410 (a)(1)(A), BA shall report to the Privacy Officer any discovery of a breach of Unsecured PHI by BA. The report shall contain the information described in Section 2(e). BA shall notify the Privacy Officer of the breach without unreasonable delay but no later than 60 days following discovery of the breach.
- b. CE Requirements. As required by 45 CFR Sections 404, 406, and 408, CE must notify affected individuals, the Secretary, and in certain circumstances, the media, following a breach of Unsecured PHI, and must do so without unreasonable delay but no later than 5 days following discovery of the breach.
  1. Notification to Affected Individuals. Pursuant to 45 CFR 164.404, CE shall notify each individual whose Unsecured PHI has been, or is reasonably believed by the BA to have been, accessed, acquired, used or disclosed as a result of the breach.
  2. Notification to the Media. Where a breach of Unsecured PHI affects more than 500 residents of a State or jurisdiction, CE shall provide notice of the breach to media outlets serving the State or jurisdiction as required under 45 CFR 164.406
  3. Notice to the Secretary. As provided in 45 CFR 164.408, CE shall notify the Secretary following the discovery of a breach.

If the breach of unsecured PHI affects more than 500 individuals, CE shall notify the Secretary of the breach without unreasonable delay, but no later than 60 days after discovery.

If the breach affects fewer than 500 individuals, CE may notify the Secretary of such breaches on an annual basis.

## 7. Term and Termination:

- a. **Term.** This Agreement shall be effective as of the Effective Date and shall continue for an initial term of one (1) year. Thereafter, this Agreement will be renewed automatically for successive one (1) year terms commencing on the first anniversary of the Effective Date and renewing annually on that date ("Renewal Date"), unless one party gives the other written notice of non-renewal at least thirty (30) days prior to the Renewal Date. Notwithstanding the term of this Agreement, however, all obligations herein shall remain in full force and effect until: (a) such time as this Agreement (including any renewals) expires or is terminated; **AND** (b) the time when all of the PHI provided by CE to BA, or created or received by BA on behalf of CE, is destroyed or returned to CE, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions of this Section.
- b. **Termination for Cause.** Upon CE's knowledge of a material breach of use and disclosure of PHI by BA, CE shall either
  - (1) Provide an opportunity for BA to cure the breach or end the violation and terminate this Agreement if BA does not cure the breach or end the violation within the time specified by CE;
  - (2) Immediately terminate this Agreement *in writing* if BA has breached a material term of this Agreement and cure is not possible; or
  - (3) if neither termination nor cure is feasible, report the violation to the **Secretary**.
- c. **Termination without Cause.** Either party may terminate this Agreement at any time for any reason, upon 30 days written notice to the other party.
- d. **Effect of Termination or Expiration of Agreement.**
  - (1) Except as provided in paragraph 2 of this Section, upon written notification of termination of this Agreement, for any reason, BA shall return or destroy all PHI received from CE, or created or received by BA on behalf of CE. This provision shall apply to PHI that is in the possession of subcontractors or agents of the BA. BA shall retain no copies of the PHI.
  - (2) In the event that BA determines that returning or destroying the PHI is infeasible, BA shall provide to CE notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make return or destruction infeasible, for so long as BA maintains such PHI.

## 8. Miscellaneous:

- a. **Regulatory references.** A reference in this Agreement to a section in the **Security and Privacy Rules** means that the section as in effect or as amended, and for which compliance is required.
- b. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the CE to comply with the requirements of the **Security and Privacy Rules** and HIPAA, Public Law 104-191.
- c. **Survival.** The respective rights and obligations of the BA under Section 6(d) of this Agreement shall survive the termination of this Agreement.

- d. Complete Agreement. This Agreement supersedes all prior and contemporaneous business associate agreements between CE and BA.
- e. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the CE to comply with the **Security and Privacy Rules.**
- f. Indemnification.
  1. The BA shall indemnify, defend, and hold CE and its directors, officers, affiliates, subsidiaries, and employees harmless from and against any and all liabilities, claims, and damages asserted against CE arising out of any breach by BA of the obligations and duties of BA under this Agreement.
  2. The CE shall indemnify, defend, and hold BA and its directors, officers, affiliates, subsidiaries, and employees harmless from and against any and all liabilities, claims, and damages asserted against BA arising out of any breach by CE of the obligations and duties of CE under this Agreement.
- g. Notification Costs related to Breaches: BA is responsible for any and all costs related to notification of individuals or next of kin (if individual is deceased) of any security or privacy breach by BA or its employees, workforce or subcontractors.

IN WITNESS WHEREOF, the parties, by their duly authorized officer, have duly executed this Agreement on the dates below.

**Sterling HSA**

By: Jean M. Campbell

By: Christine Bettner

Print Name: Jean M. Campbell

Print Name: Christine Bettner

Title: Assistant City Manager

Title: EVP, Business Development

Date: 8/5/15

Date: \_\_\_\_\_

ATTEST:  
  
 \_\_\_\_\_  
 City Clerk

Approved as to form

[Signature]  
 City Attorney