HEALTH COST HCS SOLUTIONS

BUSINESS ASSOCIATE AGREEMENT
HIPAA Protected Health Information

I. PREAMBLE

_____ ("Covered Entity") and _____ ("Business Associate") (jointly "the Parties") wish to enter into an Agreement to comply with the requirements of: (i) the implementing regulations at 45 C.F.R Parts 160, 162, and 164 for the Administrative Simplification provisions of Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (i.e., the HIPAA Privacy Rule, the HIPAA Security Standards, and the HIPAA Standards for Electronic Transactions (collectively referred to in this Agreement as "the HIPAA Regulations")), and (ii) the requirements of the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act") that are applicable to business associates, along with any guidance and/or regulations issued by the U.S. Department of Health and Human Services ("DHHS") as of September 2009. Covered Entity and Business Associate agree to incorporate into this Agreement any regulations issued by DHHS with respect to the HITECH Act that relate to the obligations of business associates and that are required to be (or should be) reflected in a business associate agreement. Business Associate recognizes and agrees that it is obligated by law to meet the applicable provisions of the HITECH Act.

II. DEFINITIONS

(a) "Electronic PHI" shall mean protected health information that is transmitted or maintained in any electronic media, as this term is defined in 45 C.F.R. § 160.103.

(b) "Limited Data Set" shall mean protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names;
- Postal address information, other than town or city, State, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

(c) "Protected Health Information" or "PHI" shall mean information created or received by a health care provider, health plan, employer, or health care clearinghouse, that: (i) relates to the past, present, or future physical or mental health or condition of an individual, provision of health care to the individual, or the past, present, or future payment for provision of health care to the individual; (ii) identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and (iii) is transmitted or maintained in an electronic medium, or in any other form or medium. The use of the term "Protected Health Information" or "PHI" in this Agreement shall mean both Electronic PHI and non-electronic PHI, unless another meaning is clearly specified.

(d) "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(e) All other terms used in this Agreement shall have the meanings set forth in the applicable definitions under the HIPAA Regulations and/or the security and privacy provisions of the HITECH Act that are applicable to business associates along with any regulations issued by the DHHS.

III. GENERAL TERMS

(a) In the event of an inconsistency between the provisions of this Agreement and a mandatory term of the HIPAA Regulations (as these terms may be expressly amended from time to time by the DHHS or as a result of interpretations by DHHS, a court, or another regulatory agency with authority over the Parties), the interpretation of DHHS, such court or regulatory agency shall prevail. In the event of a conflict among the interpretations of these entities, the conflict shall be resolved in accordance with rules of precedence.

(b) Where provisions of this Agreement are different from those mandated by the HIPAA Regulations or the HITECH Act, but are nonetheless permitted by the Regulations or the Act, the provisions of this Agreement shall control.

(c) Except as expressly provided in the HIPAA Regulations, the HITECH Act, or this Agreement, this Agreement does not create any rights in third parties.

IV. SPECIFIC REQUIREMENTS

(a) Privacy of Protected Health Information

(i) *Permitted Uses and Disclosures of PHI.* Business Associate agrees to create, receive, use, or disclose PHI only in a manner that is consistent with this Agreement or the HIPAA Privacy Rule and only in connection with providing the services to Covered Entity identified in the Agreement. Accordingly, in providing services to or for the Covered Entity, Business Associate, for example, will be permitted to use and disclose PHI for "treatment, payment, and health care operations" in accordance with the HIPAA Privacy Rule.

(1) Business Associate shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Agreement.

(2) Business Associate shall maintain safeguards as necessary to ensure that PHI is not used or disclosed except as provided for by this Agreement.

(ii) *Business Associate Obligations.* As permitted by the HIPAA Privacy Rule, Business Associate also may use or disclose PHI received by the Business Associate in its capacity as a Business Associate to the Covered Entity for Business Associate's own operations if:

(1) the use relates to: (1) the proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or (2) data aggregation services relating to the health care operations of the Covered Entity; or

(2) the disclosure of information received in such capacity will be made in connection with a function, responsibility, or services to be performed by the Business Associate, and such disclosure is required by law or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and the person agrees to notify the Business Associate of any breaches of confidentiality.

(iii) *Minimum Necessary Standard and Creation of Limited Data Set.* Business Associate's use, disclosure, or request of PHI shall utilize a Limited Data Set if practicable. Otherwise, in performing the functions and activities as specified in the Agreement and this Agreement, Business Associate agrees to use, disclose, or request only the minimum necessary PHI to accomplish the intended purpose of the use, disclosure, or request.

(iv) *Access.* In accordance with 45 C.F.R. § 164.524 of the HIPAA Privacy Rule and, where applicable, in accordance with the HITECH Act, Business Associate will make available to those individuals who are subjects of PHI, their PHI in Designated Record Sets by providing the PHI to Covered Entity (who then will share the PHI with the individual), by forwarding the PHI directly to the individual, or by making the PHI available to such individual at a reasonable time and at a reasonable location. Business Associate shall make such information available in an electronic format where directed by the Covered Entity.

(v) Disclosure Accounting. Business Associate shall make available the information necessary to provide an accounting of disclosures of PHI as provided for in 45 C.F.R. § 164.528 of the HIPAA Privacy Rule, and where so required by the HITECH Act and/or any accompanying regulations, Business Associate shall make such information available directly to the individual. Business Associate further shall provide any additional information to the extent required by the HITECH Act and any accompanying regulations.

Business Associate is not required to record disclosure information or otherwise account for disclosures of PHI that this Agreement or the Agreement in writing permits or requires: (i) for the purpose of payment activities or health care operations (except where such recording or accounting is required by the HITECH Act, and as of the effective dates for this provision of the HITECH Act), (ii) to the individual who is the subject of the PHI disclosed, or to that individual's personal representative; (iii) to persons involved in that individual's health care or payment for health care; (iv) for notification for disaster relief purposes, (v) for national security or intelligence purposes, (vi) to law enforcement officials or correctional institutions regarding inmates; (vii) pursuant to an authorization; (viii) for disclosures of certain PHI made as part of a limited data set; and (ix) for certain incidental disclosures that may occur where reasonable safeguards have been implemented.

(vi) *Amendment.* Business Associate shall make available PHI for amendment and incorporate any amendment to PHI in accordance with 45 C.F.R. § 164.526 of the HIPAA Privacy Rule.

(vii) *Right to Request Restrictions on the Disclosure of PHI and Confidential Communications.* If an individual submits a Request for Restriction or Request for Confidential Communications to the Business Associate, Business Associate and Covered Entity agree that Business Associate, on behalf of Covered Entity, will evaluate and respond to these requests according to Business Associate's own procedures for such requests.

(viii) *Return or Destruction of PHI.* Upon the termination or expiration of the Agreement or this Agreement, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or further protect the PHI if Business Associate determines that return or destruction is not feasible.

(ix) *Availability of Books and Records.* Business Associate shall make available to DHHS or its agents the Business Associate's internal practices, books, and records relating to the use and disclosure of PHI in connection with this Agreement.

(x) *Termination for Breach.*

(1) Business Associate agrees that Covered Entity shall have the right to terminate this Agreement or seek other remedies if Business Associate violates a material term of this Agreement.

(2) Covered Entity agrees that Business Associate shall have the right to terminate this Agreement or seek other remedies if Covered Entity violates a material term of this Agreement.

(b) Information and Security Standards

(i) Business Associate will develop, document, implement, maintain, and use appropriate administrative, technical, and physical safeguards to preserve the integrity, confidentiality, and availability of, and to prevent non-permitted use or disclosure of, PHI created or received for or from the Covered Entity.

(ii) Business Associate agrees that with respect to PHI, these safeguards, at a minimum, shall meet the requirements of the HIPAA Security Standards applicable to Business Associate.

(iii) More specifically, to comply with the HIPAA Security Standards for PHI, Business Associate agrees that it shall:

(1) Implement administrative, physical, and technical safeguards consistent with (and as required by) the HIPAA Security Standards that reasonably protect the confidentiality, integrity, and availability of PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall develop and implement policies and procedures that meet the Security Standards documentation requirements as required by the HITECH Act.

(2) As also provided for in Section 4(d) below, ensure that any agent, including a subcontractor, to whom it provides such PHI agrees to implement reasonable and appropriate safeguards to protect it;

(3) Report to Covered Entity, Security Incidents of which Business Associate becomes aware that result in the unauthorized access, use, disclosure, modification, or destruction of the Covered Entity's PHI, (hereinafter referred to as "Successful Security Incidents"). Business Associate shall report Successful Security Incidents to Covered Entity as specified in Section 4(e);

(4) For any other Security Incidents that do not result in unauthorized access, use, disclosure, modification, or destruction of PHI (including, for purposes of example and not for purposes of limitation, pings on Business Associate's firewall, port scans, attempts to log onto a system or enter a database with an invalid password or username, denial-of-service attacks that do not result in the system being taken off-line, or malware such as worms or viruses) (hereinafter "Unsuccessful Security Incidents"), Business Associate shall aggregate the data and, upon the Covered Entity's written request, report to the Covered Entity in accordance with the reporting requirements identified in Section 4(e);

(5) Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from a Security Incident;

(6) Permit termination of this Agreement if the Covered Entity determines that Business Associate has violated a material term of this Agreement with respect to Business Associate's security obligations and Business Associate is unable to cure the violation; and

(7) Upon Covered Entity's request, Business Associate will provide Covered Entity with access to and copies of documentation regarding Business Associate's safeguards for PHI.

(c) Compliance with HIPAA Transaction Standards

(i) *Application of HIPAA Transaction Standards.* Business Associate will conduct Standard Transactions consistent with 45 C.F.R. Part 162 for or on behalf of the Covered Entity to the extent such Standard Transactions are required in the course of Business Associate's performing services under the Agreement and this Agreement for the Covered Entity. As provided for in Section 4(d) below, Business Associate will require any agent or subcontractor involved with the conduct of such Standard Transactions to comply with each applicable requirement of 45 C.F.R. Part 162. Further, Business Associate will not enter into, or permit its agents or subcontractors to enter into, any trading partner agreement in connection with the conduct of Standard Transactions for or on behalf of the Covered Entity that:

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

(2) Adds any data element or segment to the maximum defined data set;

(3) 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

(4) Changes the meaning or intent of the Standard Transaction's implementation specification.

(ii) *Specific Communications*. Business Associate, Plan Sponsor and Covered Entity recognize and agree that communications between the parties that are required to meet the Standards for Electronic Transactions will meet the Standards set by that regulation. Communications between Plan Sponsor and Business Associate, or between Plan Sponsor and the Covered Entity, do not need to comply with the HIPAA Standards for Electronic Transactions. Accordingly, unless agreed otherwise by the Parties in writing, all communications (if any) for purposes of "enrollment" as that term is defined in 45 C.F.R. Part 162, Subpart O or for "Health Covered Entity Premium Payment Data," as that term is defined in 45 C.F.R. Part 162, Subpart Q, shall be conducted between the Plan Sponsor and either Business Associate or the Covered Entity. For all such communications (and any other communications between Plan Sponsor and the Business Associate), Plan Sponsor shall use such forms, tape formats, or electronic formats as Business Associate may approve. Plan Sponsor will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

(iii) *Communications Between the Business Associate and the Covered Entity.* All communications between the Business Associate and the Covered Entity that are required to meet the HIPAA Standards for Electronic Transactions shall do so. For any other communications between the Business Associate and the Covered Entity, the Covered Entity shall use such forms, tape formats, or electronic formats as Business Associate may approve. The Covered Entity will include all information reasonably required by Business Associate to affect such data exchanges or notifications.

(d) Agents and Subcontractors. Business Associate shall include in all contracts with its agents or subcontractors, if such contracts involve the disclosure of PHI to the agents or subcontractors, the same restrictions and conditions on the use, disclosure, and security of such PHI that are set forth in this Agreement.

(e) Breach of Privacy or Security Obligations.

(i) *Notice and Reporting to Covered Entity.* Business Associate will notify and report to Covered Entity (in the manner and within the timeframes described below) any use or disclosure of PHI not permitted by this Agreement, by applicable law, or permitted in writing by Covered Entity.

(ii) *Notice to Covered Entity.* Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than ten (10) calendar days following discovery, any "Breach" of "Unsecured Protected Health Information" as these terms are defined by the HITECH Act and any implementing regulations. Business Associate shall cooperate with Covered Entity in investigating the Breach and in meeting the Covered Entity's obligations under the HITECH Act and any other security breach notification laws. Business Associate shall follow its notification to the Covered Entity with a report that meets the requirements outlined immediately below.

(iii) *Reporting to Covered Entity.*

(1) For Successful Security Incidents and any other use or disclosure of PHI that is not permitted by this Agreement, the Agreement, by applicable law, or without the prior written approval of the Covered Entity, Business Associate – without unreasonable delay and in no event later than thirty (30) days after Business Associate learns of such non-permitted use or disclosure – shall provide Covered Entity a report that will:

a. Identify (if known) each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach;
b. Identify the nature of the non-permitted access, use, or disclosure including the date of the incident and the date of discovery;
c. Identify the PHI accessed, used, or disclosed (e.g., name; social security number; date of birth);
d. Identify who made the non-permitted access, use, or received the non-permitted disclosure;
e. Identify what corrective action Business Associate took or will take to prevent further non-permitted accesses, uses, or disclosures;
f. Identify what Business Associate did or will do to mitigate any deleterious effect of the non-permitted access, use, or disclosure; and
g. Provide such other information, including a written report, as the Covered Entity may reasonably request.

(2) For Unsuccessful Security Incidents, Business Associate shall provide Covered Entity, upon its written request, a report that: (i) identifies the categories of Unsuccessful Security Incidents as described in Section 4(b)(iii)(4); (ii) indicates whether Business Associate believes its current defensive security measures are adequate to address all Unsuccessful Security Incidents, given the scope and nature of such attempts; and (iii) if the security measures are not adequate, the measures Business Associate will implement to address the security inadequacies.

(iv) *Termination for Breach.*

(1) Covered Entity and Business Associate each will have the right to terminate this Agreement if the other party has engaged in a pattern of activity or practice that constitutes a material breach or violation of Business Associate's or the Covered Entity's respective obligations regarding PHI under this Agreement and, on notice of such material breach or violation from the Covered Entity or Business Associate, fails to take reasonable steps to cure the material breach or end the violation.

(2) If Business Associate or the Covered Entity fail to cure the material breach or end the violation after the other party's notice, the Covered Entity or Business Associate (as applicable) may terminate this Agreement by providing Business Associate or the Covered Entity written notice of termination, stating the uncured material breach or violation that provides the basis for the termination and specifying the effective date of the termination. Such termination shall be effective 60 days from this termination notice.

(v) *Continuing Privacy and Security Obligations.* Business Associate's and the Covered Entity's obligation to protect the privacy and security of the PHI it created, received, maintained, or transmitted in connection with services to be provided under the Agreement and this Agreement will be continuous and survive termination, cancellation, expiration, or other conclusion of this Agreement or the Agreement. Business Associate's other obligations and rights, and the Covered Entity's obligations and rights upon termination, cancellation, expiration, or other conclusion of this Agreement, are those set forth in this Agreement and/or the Agreement.

V. TERMS

This Agreement is effective as of the date upon which signatures are affixed. This Agreement shall be in effect for three (3) years from the effective date. This Agreement shall then automatically renew for additional one-year terms unless either party gives notice to the other at least 90 days before the end of the next expiration date of its decision not to renew this Agreement.

AGREED AND UNDERSTOOD:

Covered Entity:	**Business Associate:**
_____	_____
SIGNATURE	SIGNATURE
TITLE: _____	TITLE: _____
DATE: _____	DATE: _____