



**BUSINESS ASSOCIATE AGREEMENT
BETWEEN COUNTY OF TEHAMA
and
SELF INSURED SERVICES COMPANY dba BENEFIT COORDINATORS CORPORATION**

1. PREAMBLE

County of Tehama ("Covered Entity"), with a business address at 727 Oak Street, Red Bluff, CA 96080, and Self Insured Services Company, LLC doing business as Benefit Coordinators Corporation ("Business Associate), with a business address at 2 Robinson Plaza, Suite 200, Pittsburgh, Pennsylvania 15205, (jointly "the Parties") enter into this Business Associate 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, Security, Electronic Transaction, Breach Notification, and Enforcement Rules ("the Implementing Regulations")),
- (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, and
- (iii) The requirements of the final modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules as issued on January 25, 2013 and effective March 26, 2013 (75 Fed. Reg. 5566 (Jan. 25, 2013)) ("the Final Regulations"). The Implementing Regulations, the HITECH Act, and the Final Regulations are collectively referred to in this Business Associate Agreement as "the HIPAA Requirements."

Covered Entity and Business Associate agree to incorporate into this Business Associate Agreement any regulations issued by the U.S. Department of Health and Human Services ("DHHS") with respect to the HIPAA Requirements 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 HIPAA Requirements and that it has direct liability for any violations of the HIPAA Requirements.

2. DEFINITIONS

- a) "*Breach*" shall mean, as defined in 45 C.F.R. § 164.402, the acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted by the HIPAA Requirements that compromises the security or privacy of that Protected Health Information.
- b) "*Business Associate Subcontractor*" shall mean, as defined in 45 C.F.R. § 160.103, any entity (including an agent) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate.
- c) "*Electronic PHI*" shall mean, as defined in 45 C.F.R. § 160.103, Protected Health Information that is transmitted or maintained in any Electronic Media.
- d) "*Limited Data Set*" shall mean, as defined in 45 C.F.R. § 164.514(e), Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
 - i.) Names;
 - ii.) Postal address information, other than town or city, State, and zip code;
 - iii.) Telephone numbers;

- iv.) Fax numbers;
 - v.) Electronic mail addresses;
 - vi.) Social security numbers;
 - vii.) Medical record numbers;
 - viii.) Health plan beneficiary numbers;
 - ix.) Account numbers;
 - x.) Certificate/license numbers;
 - xi.) Vehicle identifiers and serial numbers, including license plate numbers;
 - xii.) Device identifiers and serial numbers;
 - xiii.) Web Universal Resource Locators (URLs);
 - xiv.) Internet Protocol (IP) address numbers;
 - xv.) Biometric identifiers, including finger and voice prints; and
 - xvi.) Full face photographic images and any comparable images.
- e) “*Protected Health Information*” or “*PHI*” shall mean, as defined in 45 C.F.R. § 160.103, 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 Business Associate Agreement shall mean both Electronic PHI and non-Electronic PHI, unless another meaning is clearly specified.

- f) “*Security Incident*” shall mean, as defined in 45 C.F.R. § 164.304, the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- g) “*Unsecured Protected Health Information*” shall mean, as defined in 45 C.F.R. § 164.402, Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by DHHS.
- h) All other capitalized terms used in this Business Associate Agreement shall have the meanings set forth in the applicable definitions under the HIPAA Requirements.

3. GENERAL TERMS

- (a) In the event of an inconsistency between the provisions of this Business Associate Agreement and a mandatory term of the HIPAA Requirements (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 Business Associate Agreement are different from those mandated by the HIPAA Requirements, but are nonetheless permitted by the HIPAA Requirements, the provisions of this Business Associate Agreement shall control.

- (c) Except as expressly provided in the HIPAA Requirements or this Business Associate Agreement, this Business Associate Agreement does not create any rights in third parties.

4. SPECIFIC REQUIREMENTS

- a) Flow-Down of Obligations to Business Associate Subcontractors. Business Associate agrees that as required by the HIPAA Requirements, Business Associate will enter into a written agreement with all Business Associate Subcontractors that:
- i.) Requires them to comply with the Privacy and Security Rule provisions of this Business Associate Agreement in the same manner as required of Business Associate, and
 - ii.) Notifies such Business Associate Subcontractors that they will incur liability under the HIPAA Requirements for non-compliance with such provisions. Accordingly, Business Associate shall ensure that all Business Associate Subcontractors agree in writing to the same privacy and security restrictions, conditions and requirements that apply to Business Associate with respect to PHI.
- b) Privacy of Protected Health Information
- i.) *Permitted Uses and Disclosures of PHI.* Business Associate agrees to create, receive, use, disclose, maintain or transmit PHI only in a manner that is consistent with this Business Associate Agreement or the HIPAA Requirements and only in connection with providing the services to Covered Entity identified in the underlying administrative services agreement (“the Service 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,” as those terms are defined in the HIPAA Requirements. Business Associate further agrees that to the extent it is carrying out one or more of the Covered Entity’s obligations under the Privacy Rule (Subpart E of 45 C.F.R. Part 164), it shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.
 - (1) Business Associate shall report to Covered Entity any use or disclosure of PHI that is not provided for in this Business Associate Agreement, including reporting Breaches of Unsecured Protected Health Information as required by 45 C.F.R. § 164.410 and required by Section 4(e)(ii) below.
 - (2) Business Associate shall establish, implement and maintain appropriate safeguards, and comply with the Security Standards (Subpart C of 45 C.F.R. Part 164) with respect to Electronic PHI, as necessary to prevent any use or disclosure of PHI other than as provided for by this Business Associate Agreement.
 - (3) Business Associate agrees that to the extent it receives records that are subject to 42 C.F.R. Part 2 (“Part 2”), Business Associate shall comply with the requirements of Part 2 in the handling of such records, including implementation, maintenance and use of appropriate safeguards to prevent unauthorized use or disclosure of Part 2 information and reporting of any unauthorized use, disclosure or breach of Part 2 information to the Covered Entity within ten (10) calendar days of discovery of such unauthorized use, disclosure or breach.
 - ii.) *Business Associate Obligations.* As permitted by the HIPAA Requirements, 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:
 - (a) The proper management and administration of the Business Associate or to carry out legal responsibilities of the Business Associate, or
 - (b) 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 Service Agreement and this Business Associate 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 Requirements, Business Associate will make available to the Covered Entity (or as directed by the Covered Entity, to those individuals who are the subject of the PHI (or their designees)), their PHI in the Designated Record Set. 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 Requirements by making such information available to the Covered Entity or (at the direction of the Covered Entity) making such information available directly to the individual.
- vi.) *Amendment.* Business Associate shall make PHI in a Designated Record Set available for amendment and, as directed by the Covered Entity, incorporate any amendment to PHI in accordance with 45 C.F.R. § 164.526 of the HIPAA Requirements.
- 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 Service Agreement or this Business Associate Agreement, Business Associate agrees to return the PHI to Covered Entity, destroy the PHI (and retain no copies), or if Business Associate determines that return or destruction of the PHI is not feasible,
- (1) Continue to extend the protections of this Business Associate Agreement and of the HIPAA Requirements to the PHI, and
- (2) Limit any further uses and disclosures of the PHI to the purpose making return or destruction infeasible.
- 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 Business Associate Agreement.
- x.) *Termination for Breach.*
- (1) Business Associate agrees that Covered Entity shall have the right to terminate this Business Associate Agreement or seek other remedies if Business Associate violates a material term of this Business Associate Agreement.
- (2) Covered Entity agrees that Business Associate shall have the right to terminate this Business Associate Agreement or seek other remedies if Covered Entity violates a material term of this Business Associate Agreement.

c) 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, Electronic PHI created or received for or from the Covered Entity.
- ii.) Business Associate agrees that with respect to Electronic 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 Electronic 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 Electronic 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 documentation requirements as required by the HIPAA Requirements;
 - (2) As also provided for in Section 4(a) above, ensure that any Business Associate Subcontractor agrees to implement reasonable and appropriate safeguards to protect the Electronic PHI;
 - (3) Report to Covered Entity any unauthorized access, use, disclosure, modification, or destruction of PHI (including Electronic PHI) not permitted by this Business Associate Agreement, applicable law, or permitted by Covered Entity in writing ("Successful Security Incidents" or Breaches) of which Business Associate becomes aware. Business Associate shall report such Successful Security Incidents or Breaches to Covered Entity as specified in Section 4(e)(iii)(1);
 - (4) For 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"). This Agreement constitutes notification of any Unsuccessful Security Incidents. The parties acknowledge and agree that no further notice of Unsuccessful Security Incidents will be required;
 - (5) Take all commercially reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate resulting from any unauthorized access, use, disclosure, modification, or destruction of PHI;
 - (6) Permit termination of this Business Associate Agreement if the Covered Entity determines that Business Associate has violated a material term of this Business Associate 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, provide Covered Entity with access to and copies of documentation regarding Business Associate's safeguards for PHI and Electronic PHI.

d) 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 Service Agreement and this Business Associate Agreement for the Covered Entity. As provided for in Section 4(a) above, Business Associate will require any Business Associate 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 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.) *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.

e) Notice and Reporting Obligations of Business Associate

- i.) *Notice of Non-Compliance with the Business Associate Agreement.* Business Associate will notify Covered Entity within 10 calendar days after discovery, any unauthorized access, use, disclosure, modification, or destruction of PHI (including any successful Security Incident) that is not permitted by this Business Associate Agreement, by applicable law, or permitted in writing by Covered Entity, whether such non-compliance is by (or at) Business Associate or by (or at) a Business Associate Subcontractor.
- ii.) *Notice of Breach.* Business Associate will notify Covered Entity following discovery and without unreasonable delay but in no event later than 10 calendar days following discovery, any Breach of Unsecured Protected Health Information, whether such Breach is by Business Associate or by Business Associate Subcontractor.
- (1) As provided for in 45 C.F.R. § 164.402, Business Associate recognizes and agrees that any acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule (Subpart E of 45 C.F.R. Part 164) is presumed to be a Breach. As such, Business Associate shall (i) notify Covered Entity of any non-permitted acquisition, access, use or disclosure of PHI, and (ii) assist Covered Entity in performing (or at Covered Entity's direction, perform) a risk assessment to determine if there is a low probability that the PHI has been compromised.
 - (2) Business Associate shall cooperate with Covered Entity in meeting the Covered Entity's obligations under the HIPAA Requirements 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 Obligations.*

- (1) For Successful Security Incidents and Breaches, Business Associate – without unreasonable delay and in no event later than 20 calendar days after Business Associate learns of such non-permitted use or disclosure (whether at Business Associate or at Business Associate Subcontractor) – 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;
 - (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 what corrective action Business Associate (or Business Associate Subcontractor) took or will take to prevent further non-permitted accesses, uses, or disclosures;
 - (e) Identify what Business Associate (or Business Associate Subcontractor) did or will do to mitigate any deleterious effect of the non-permitted access, use, or disclosure; and
 - (f) Provide such other information, including a written report, as the Covered Entity may reasonably request.
- (2) For Unsuccessful Security Incidents, this Agreement constitutes notification of any unsuccessful Security Incidents. The parties acknowledge and agree that no further notice of unsuccessful Security Incidents will be required.

iv.) *Termination.*

- (1) Covered Entity and Business Associate each will have the right to terminate this Business Associate 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 Business Associate 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 Business Associate 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 Service Agreement and this Business Associate Agreement will be continuous and survive termination, cancellation, expiration, or other conclusion of this Business Associate Agreement or the Service 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 Business Associate Agreement, are those set forth in this Business Associate Agreement and/or the Service Agreement.

IN WITNESS WHEREOF, each of the undersigned has caused this Business Associate Agreement to be duly executed in its name and on its behalf, effective as of the last date of signature by a party hereto.

**Self Insured Services Company, LLC dba
Benefit Coordinators Corporation**

County of Tehama

Signature of Privacy Officer

Nicole Ames

Name, printed

HIPAA Privacy Officer

Title

Date signed

Signature of Officer

Name, printed

Title

Date signed