

<b>CHELAN-DOUGLAS RSN/PHP POLICY AND PROCEDURE MANUAL</b>		Chapter:	1.4.2.23
Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Page:	1 of 14
		Date Effective:	April 14, 2003
Subject:	Uses and Disclosures - Business Associates	Date Revised:	March 9, 2011
		Authorizing Signature:	

**AUTHORITY:** Authorizing Source: RCW 70.02  
45 CFR § 164.504, 45 CFR §164.501, 45 CFR §164.524, 45 CFR §164.526, 45 CFR §164.528  
ARRA Title XIII Section 13402 - "Notification in the Case of Breach"

**SCOPE:** This policy applies to Chelan-Douglas Regional Support Network/Prepaid Inpatient Health Plan (CDRSN/PIHP) and its contractors (agencies/providers), subcontractors (referred to as contractors or agencies or providers throughout this policy), and Business Associates.

**PURPOSE:** To delineate the nature of the Business Associate relationship and to demarcate the obligations of CDRSN and Business Associates relative to the use, disclosure and safeguarding of Protected Health Information.

**DEFINITIONS:** "Breach" means: The same meaning as the term "breach" in §13400 of the HITECH Act and shall include the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information.

"Business Associate" means:

(1) With respect to a covered entity, a person who:

- (a) On behalf of such Covered Entity or of an Organized Health Care Arrangement (as defined in §164.501 of this subchapter), in which the Covered Entity participates, but other than in the capacity of a member of the Workforce of such Covered Entity or Arrangement, performs, or assists in the performance of:
  - (i) A function or activity involving the Use or Disclosure of Individually Identifiable Health Information, including claims processing or administration, data analysis, processing or administration, utilization

review, quality assurance, billing, benefit management, practice management, and repricing; or

- (ii) Any other function or activity regulated by this Policy; or
  - (b) Provides, other than in the capacity of a member of the Workforce of such Covered Entity, legal, actuarial, accounting, consulting, Data Aggregation (as defined in 45 CFR §164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an Organized Health Care Arrangement in which the Covered Entity participates, where the provision of the service involves the Disclosure of Individually Identifiable Health Information from such Covered Entity or Arrangement, or from another business associate of such Covered Entity or Arrangement, to the person.
- (2) A covered entity participating in a Organized Health Care Arrangement that performs a function or activity as described by Paragraph (1)(a) of this definition for or on behalf of such Organized Health Care Arrangement, or that provides a service as described in Paragraph (1)(b) of this definition to or for such Organized Health Care Arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a Business Associate or other covered entities participating in such Organized Health Care Arrangement.
- (3) A covered entity may be the Business Associate of another covered entity.

"Designated Record Set" means: The same meaning as the term "designated record set" in 45 CFR §164.501.

"Privacy Rule" means: The Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E, as amended by the HITECH Act and as may otherwise be amended from time to time.

"Protected Health Information" (PHI) means: Individually identifiable health information:

- (1) Except as provided in paragraph 2 of this definition, that is:
  - (a) Transmitted by electronic media;

- (b) Maintained in any medium described in the definition of electronic media in 45 CFR 162.103; or
- (c) Transmitted or maintained in any other form

(2) PHI excludes individually identifiable health information in:

- (a) Education records covered by the Family Educational Rights and Privacy Act
- (b) Records described in 20 USC 1232g(a)(4)(B)(iv)

"Required by Law" means: The same meaning as the term "required by law" in 45 CFR §164.501.

"Secretary" means: The Secretary of the U.S. Department of Health and Human Services.

"Unsecured Protected Health Information" means: PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance or as otherwise defined in §13402(h) of the HITECH Act.

**POLICY:**

Prior to disclosing any Protected Health Information to a Business Associate of CDRSN, CDRSN will obtain satisfactory assurances from a Business Associate that the Business Associate will appropriately safeguard the Protected Health Information it receives or creates on behalf of CDRSN. CDRSN will document these satisfactory assurances in writing in the form of a Business Associate Agreement with the Business Associate in compliance with the HIPAA and HITECH Act regulations. Any disclosures to a Business Associate must be limited to disclosures permitted by the HIPAA regulations and not for the Business Associate's independent use or purposes.

**PROCEDURE:**

**I. Determining if a Person of Entity is a Business Associate**

- (1) Based upon the definition of "Business Associate" as stated in this Policy, a Business Associate is not an employee of the CDRSN.
- (2) For each person or entity with whom the CDRSN contracts or is otherwise engages in business, other than CDRSN employees, the CDRSN Business Associate Assessment (see Attachment 1) shall be completed to determine whether the individual or entity meets the definition of Business Associate.

- (2) Persons or entities determined to meet the definition of a Business Associate shall be required to comply with CDRSN Policies and Procedures related to Business Associates, as well as applicable HIPAA security and privacy regulations.

## II. Disclosures to a Business Associate

- (1) CDRSN may not disclose PHI to a Business Associate or allow a Business Associate to create or receive PHI on behalf of CDRSN until:
  - (a) CDRSN obtains satisfactory assurance that the Business Associate will appropriately maintain the confidentiality of the PHI using appropriate Administrative, Physical and Technical safeguards, as required by HIPAA regulations; and
  - (b) CDRSN receives documentary evidence of Business Associate's internal policies and procedures for ensuring compliance with obligations delineated in the Business Associate Agreement.

## III. Disclosures to the Business Associate of Another Covered Entity

- (1) CDRSN may share PHI directly with the Business Associate acting on behalf of another covered entity, provided the disclosure is one that is permitted by HIPAA.

## IV. Disclosure of Only the Minimum Necessary

- (1) CDRSN will disclose to a Business Associate only the PHI that is reasonably necessary to accomplish the intended purpose of the disclosure.
- (2) The Business Associate must request only the information that is the minimum necessary, and therefore, CDRSN may reasonably rely on a request from a Business Associate, or the Business Associate of another covered entity, to be a request for PHI that meets the minimum necessary standards.

## V. Disclosures Through Limited Data Sets

- (1) When CDRSN discloses information to a Business Associate through the use of a limited data set pursuant to CDRSN Policy and Procedure 1.4.2.7 "De-identification and Limited Data Sets" a

Business Associate Agreement is not required.

## VI. Business Associate Agreements

- (1) If a person or entity meets the definition of a "Business Associate," a Business Associate Agreement is required to document the assurances from the Business Associate that the Business Associate will appropriately safeguard the PHI it receives or creates on behalf of CDRSN.
- (2) The Business Associate Agreement between CDRSN and a Business Associate shall:
  - (a) Establish the permitted and required uses and disclosures of PHI by the Business Associate on behalf of CDRSN;
  - (b) Prohibit a Business Associate from the use or further disclosure of PHI in a manner that would violate the HIPAA Privacy Rule if such use were done by CDRSN;
  - (c) Authorize CDRSN to terminate the Business Associate Agreement if CDRSN determines that the Business Associate has violated a material term of the Business Associate Agreement;
  - (d) Provide that the Business Associate Shall:
    - (i) Not use or disclosure PHI other than as permitted or required by the Business Associate Agreement or as required by law;
    - (ii) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of the CDRSN;
    - (iii) Immediately notify CDRSN of any use or disclosure of PHI in violation of the Business Associate Agreement;
    - (iv) Promptly notify CDRSN of a breach of unsecured PHI following the first day on which the Business Associate (or Business Associate's employee, office or agent) knows of such a breach or following the first day on which the Business Associate (or Business

Associate's employee, office or agent) should have known of such breach. Notification shall:

- (A) Be made to the CDRSN no later than 60 calendar days after discovery of the breach, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security; and
  - (B) Include the individuals whose unsecured PHI has been, or is reasonably believed to have been, the subject of a breach;
- (v) In the event of an unauthorized use or disclosure of PHI or a breach of unsecured PHI, mitigate, to the extent practicable, any harmful effects of said disclosure that are known to it;
  - (vi) Ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of the CDRSN, agrees to the same restrictions and conditions that apply through this section;
  - (vii) Require that, to the extent applicable, the Business Associate shall provide access to PHI in a Designated Record Set at reasonable times, at the request of CDRSN or, as directed by CDRSN, to an individual in order to meet the requirements of 45 CFR §164.524;
  - (viii) Require that, to the extent applicable, the Business Associate shall make any amendment(s) to PHI in a Designated Record Set that CDRSN directs or agrees to pursuant to 45 CFR §164.526 at the request of CDRSN or an individual;
  - (ix) Upon request with reasonable notice provide CDRSN access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI;
  - (x) Agree to document such disclosures of PHI and information related to such disclosures as would be required for a Covered Entity to respond to a request by an individual for an accounting of disclosures of

PHI in accordance with 45 CFR §164.528. Should an individual make a request to CDRSN for an accounting of disclosures of his or her PHI pursuant to 45 CFR §164.528, Business Associate shall agree to promptly provide CDRSN with information in a format and manner sufficient to respond to the individual's request;

- (xi) Upon request with reasonable notice provide CDRSN with an accounting of uses and disclosures of PHI;
  - (xii) Make its internal practices, books, records, and any other material requested by the Secretary relating to the use, disclosure, and safeguarding of PHI received from CDRSN available to the Secretary for the purpose of determining compliance with the Privacy Rule. The aforementioned information shall be made available to the Secretary in a manner and place as designated by the Secretary or the Secretary's duly appointed delegate. The Business Associate shall comply and cooperate with any request for documents or other information from the Secretary directed to CDRSN that seeks documents or other information held by the Business Associate.
- (e) Provide that the Business Associate may:
- (i) Use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1); and
  - (ii) Except as otherwise limited in this Policy and Procedure, disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances 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 Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- (f) Provide that upon termination of the Business Associate agreement with CDRSN, the Business Associate shall return

or destroy all PHI received from CDRSN, or created or received by the Business Associate on behalf of CDRSN, that the Business Associate still maintains in any form and retain no copies of such information; or, if such return or destruction is not feasible, the obligations of the Business Associate contained in the Business Associate Agreement shall extend beyond termination of the agreement for so long as the Business Associate maintains such PHI.

- (3) The Business Associate Agreement may permit the Business Associate to use PHI received by the Business Associate in its capacity as a Business Associate to CDRSN, only if such use is necessary for:
  - (a) The proper management and administration of the Business Associate; or
  - (b) To carry out the legal responsibilities of the Business Associate.
- (4) The Business Associate Agreement may permit the Business Associate to disclose PHI received by the Business Associate in its capacity as a Business Associate to CDRSN, only if such disclosure is necessary for:
  - (a) The proper management and administration of the Business Associate; or
  - (b) To carry out the legal responsibilities of the Business Associate.
- (5) Prior to any disclosure by a Business Associate, the following must occur:
  - (a) The Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially 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 Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

## VII. Non-Compliance of Business Associate

- (1) If CDRSN has actual knowledge of a pattern of activity or practice of the Business Associate that constitutes a material breach or

violation of an obligation of the Business Associate under the Business Associate Agreement, CDRSN shall take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, CDRSN must:

- (a) Terminate the Business Associate Agreement, if feasible; or if the termination is not feasible, report the problem to the Secretary for the United States Department of Health and Human Services; and
- (b) Mitigate, to the extent practicable, any harmful effect that is known to CDRSN arising from a disclosure of PHI in violation of the CDRSN Policies and Procedures or the HIPAA regulations.

#### VIII. Transitioning from Existing Contracts

- (1) Contracts and agreements in force as of the effective date of this Policy and Procedure shall be reviewed using the CDRSN Business Associate Assessment to determine whether the person or entity with whom the contract of agreement is held qualifies as a Business Associate.
- (2) Persons or entities with whom CDRSN current contracts or has agreements and who are identified as meeting the definition of Business Associate, and for whom a Business Associate Agreement consistent with this Policy and Procedure has not been executed, shall receive updated Business Associate Agreements to be executed within 30 days of notice by CDRSN, or as allowable under the existing contract or agreement.
- (3) Prior to the execution of new Business Associate Agreements, CDRSN must ensure, in whatever reasonable manner deemed effective by CDRSN, the appropriate cooperation by its Business Associates in meeting the following requirements during the transition period:
  - (a) Make information available to the Secretary, including information held by a Business Associate, as necessary for the Secretary to determine compliance by CDRSN;
  - (b) Fulfill an individual's rights to access and amend his or her PHI contained in a Designated Record Set, including information held by a Business Associate, if appropriate, and receive an accounting of disclosures by a Business Associate;

- (c) Mitigate, to the extent practicable, any harmful effect that is known to CDRSN or an impermissible use or disclosure of PHI by its Business Associate;

# BUSINESS ASSOCIATE ASSESSMENT FOR CDRSN

For Use in Identifying CDRSN Business Associate Relationships with a Public/Private Contractor or Vendor.

## Section One: Introduction

**HIPAA Business Associate:** A person or organization that performs a function or activity for, or on behalf of a HIPAA covered health care component or that provides certain legal, financial, or management services to a covered health care component; wherein such services involve the sharing of individually identifiable health information.

## Section Two: Instructions

1. Complete this **Business Associate Assessment** for every **contract** with a public or private contractor or vendor.
2. If it is determined that a business associate relationship exists, any contract or agreement must meet the business associate requirements of 45 CFR 164 and the HITECH Act
3. If there are questions about the privacy relationship of a service provider with the agency, the CDRSN Privacy Officer will make the determination as to whether the contractor or vendor is a business associate
4. If no business associate relationship exists, process the MOU or contract in the usual manner.

## Section Three: General Information

Contractor/Vendor	
Contract/Agreement Number	
Agency Contract Administrator	
Date Assessment Completed	

**Section Four: Assessment of Service Provided by Public or Private Contractor**

<p>1. Has a relationship been initiated that allows a public or private contractor to perform a function or activity for, or on behalf of a CDRSN HIPAA covered health care component?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Name of Contractor</p> <p>_____</p> <p>_____</p> <p>Service Provided</p> <p>_____</p> <p>_____</p>	<p>Yes – Go to Question 2.</p> <p>No – Stop. There is no business associate relationship.</p>
<p>2. Is the function or service to be rendered by a public or private contractor an activity <b>other than treatment</b> of clients?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: The sharing of individually identifiable health information with another treatment provider for treatment purposes only does not require a business associate agreement.</p>	<p>Yes – Go to Question 3.</p> <p>No – Stop. There is no business associate relationship.</p>
<p>3. Does the function or service to be rendered by a public or private contractor involve the use or disclosure of individually identifiable health information?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: Data that does not contain individually identifiable health information does not have to be protected through a business associate agreement.</p>	<p>Yes – Go to Question 4.</p> <p>No – Stop. There is no business associate relationship.</p>
<p>4. Are the services rendered by a public or private contractor performed <b>on the premises</b> of a CDRSN HIPAA covered health care provider, using that provider's resources and following that provider's policies and procedures?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: Whenever a service is rendered on the premises of a CDRSN HIPAA covered provider, utilizing that provider's office and supplies and following that provider's requirements, the person rendering such services is considered a member of that provider's workforce, and is therefore required to comply with that provider's privacy policies and procedures.</p>	<p>No – Go to Question 5.</p> <p>Yes – Stop. There is no business associate relationship.</p>
<p>5. Is the type(s) of function/activity to be rendered by a public or</p>	<p>Check appropriate service(s):</p> <p><b>Legal</b></p> <p><input type="checkbox"/> Attorney Representing Agency</p>	<p><b>Yes - Business Associate Identified</b></p>

**Section Four: Assessment of Service Provided by Public or Private Contractor**

<p>private contractor to the CDRSN covered health care component listed in column 2?</p> <p><input type="checkbox"/> Yes – See column 2  <input type="checkbox"/> No – Activity Listed below</p> <hr/> <hr/>	<p><b><u>Actuarial</u></b>  <input type="checkbox"/> Benefits Management</p> <p><b><u>Accounting</u></b>  <input type="checkbox"/> Patient Accounts Billing  <input type="checkbox"/> Claims Processing  <input type="checkbox"/> Claims Administration  <input type="checkbox"/> Bill Collections</p> <p><b><u>Consulting</u></b>  <input type="checkbox"/> Professional Services  <input type="checkbox"/> Special Population Assessments</p> <p><b><u>Data Aggregation Services</u></b>  <input type="checkbox"/> Data Analysis  <input type="checkbox"/> Data Processing  <input type="checkbox"/> Data Administration</p> <p><b><u>Accreditation Services</u></b>  <input type="checkbox"/> JCAHO  <input type="checkbox"/> Council on Accreditation</p> <p><b><u>Financial Services</u></b>  <input type="checkbox"/> Re-pricing  <input type="checkbox"/> Rate Setting</p> <p><b><u>Management Services</u></b>  <input type="checkbox"/> Practice Management  <input type="checkbox"/> Software Support  <input type="checkbox"/> Utilization Review  <input type="checkbox"/> Quality Assurance Contract Analysis  <input type="checkbox"/> Central Office Supervision</p> <p><b><u>Administrative Services</u></b>  <input type="checkbox"/> Security  <input type="checkbox"/> Dietary  <input type="checkbox"/> Machine Maintenance  <input type="checkbox"/> Facility Maintenance  <input type="checkbox"/> Landscaping  <input type="checkbox"/> Housekeeping  <input type="checkbox"/> Hardware Support  <input type="checkbox"/> Audits/Surveys  <input type="checkbox"/> Purchasing</p>	<p>Note: The specified function/activity, which involves the sharing of individually identifiable health information, is to be provided by a public or private contractor. This constitutes an External Business Associate relationship and such information must be protected. Therefore, a Business Associate Agreement or Addendum must be developed and attached to the CDRSN contract with the contractor or vendor identified above.</p> <p>No – Stop. There is no business associate relationship.</p>
--	--	---

**Section Five: Additional Requirements Regarding Business Associates**

<p>1. Has the Agency Privacy Officer been notified of this business associate relationship?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: The Agency Privacy Officer needs to be notified of all services provided by a business associate. Notification may be accomplished through e-mail.</p>	<p>Yes – Go to Question 2.</p> <p>No - Stop. Business associate relationship was not established.</p>
<p>2. Has the Business Associate provided documentation on internal procedures for complying with obligations Business Associate Agreement?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: CDRSN Privacy Policy "Uses and Disclosures: Business Associate" requires business associates to provide "documentary evidence of Business Associate's internal policies and procedures for ensuring compliance with obligations delineated in the Business Associate Agreement" to the CDRSN Privacy Officer.</p>	<p>Yes – Go to Question 3.</p> <p>No – Stop. Business associate relationship was not established.</p>
<p>3. Has the contracts spreadsheet been updated to indicate a business associate relationship with this business associate?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Note: The contracts spreadsheet, which accounts for the "purchase" of a service, includes a box to be checked whenever a CDRSN MOU or Contract has a Business Associate Agreement attached to it. This element allows for tracking of CDRSN Business Associates.</p>	<p>Yes – Business Associate relationship has been properly acknowledged.</p> <p>No – Stop. There is no business associate relationship.</p>

\*\*\*End of Document\*\*\*