

<b>CHELAN-DOUGLAS RSN/PIHP POLICY AND PROCEDURE MANUAL</b>		Chapter:	1.4.2.2
Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Page:	1 of 3
		Date Effective:	April 14, 2003
Subject:	Administrative Requirements for the Implementation of HIPAA	Date Revised:	April 14, 2003
		Date Revised:	June 1, 2009
		Date Revised:	February 23, 2011
		Authorizing Signature:	

**AUTHORITY:** Authorizing Source: RCW 70.02 45 CFR 165 (HIPAA)

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

**PURPOSE:** To issue instructions regarding the Chelan-Douglas Regional Support Network's obligations relating to the implementation of the Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. §§ 1320d-1329d-8, and regulations promulgated there under, 45 CFR Parts 160, 162 and 164.

**DEFINITIONS:** See 1.3.2.0

**POLICY:**

- A. Personnel Designations: The CDRSN must designate and document designations of the following:
  - Privacy Officer: The CDRSN will designate an individual to be the Privacy Officer, responsible for the development and implementation of CDRSN-wide policies and procedures relating to the safeguarding of PHI.
  - This individual, position title, or office will be responsible for receiving complaints relating to PHI and for providing information about the entity's privacy practices. The Privacy Officer may designate staff to perform this function when the Privacy Officer is absent or unavailable,
  
- B. Training Requirements: The CDRSN and, as applicable, its offices, programs and facilities, must document the following training actions:
  - All CDRSN employees and other workforce members must receive training on applicable policies and procedures relating to PHI as necessary and appropriate for such persons to carry out their functions.

- Each new workforce member shall receive the training as described above within a reasonable time after joining the workforce.
  - Each workforce member whose functions are impacted by a material change in the policies and procedures relating to PHI, or by a change in position or job description, must receive the training as described above within a reasonable time after the change becomes effective.
- C. Safeguards: Each office, program or facility of the CDRSN, as well as Business Associates affiliated with the CDRSN or contracted providers, must have in place appropriate administrative, technical, and physical safeguards to reasonably safeguard PHI from intentional or unintentional unauthorized use or disclosure.
- D. Complaint Process: Each office of the CDRSN must have in place a process for individuals to make complaints about the entity's HIPAA policies and procedures and/or the entity's compliance with those policies and procedures, and must document all complaints received and the disposition of each complaint.
- E. Sanctions: The applicable Human Resources Office for every office, program or facility of the CDRSN must have in place, must apply and must document application of appropriate sanctions against workforce members who fail to comply with HIPAA policies and procedures. [Note - there are exceptions for disclosures made by workforce members who qualify as whistleblowers or certain crime victims.]
- F. Mitigation Efforts Required: Each office, program or facility must mitigate, to the extent practicable, any harmful effects of unauthorized uses or disclosures of PHI by the entity or any of its business associates.
- G. Breach Notification: Each office, program or facility of the CDRSN, as well as Business Associates affiliated with the CDRSN or contracted providers, shall have Policies and Procedures in place to ensure compliance with the Breach Notification rule of the HITECH Act.
- H. Intimidating or Retaliatory Acts and Waiver of Rights Prohibited:
- Prohibition on Intimidating or Retaliatory Acts: Neither the CDRSN nor any office, program, facility or workforce member shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA

compliance, or against any person for filing a complaint with the Secretary of the U.S. CDRSN of Health and Human Services, participating in a HIPAA related investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under HIPAA regulations as long as the action does not involve disclosure of PIHP in violation of the regulations.

- Prohibition on Waiver of Rights: No office, program, facility or workforce member of the CDRSN shall require individuals to waive any of their rights under HIPAA as a condition of treatment, payment, and enrollment in a health plan or eligibility for benefits.
- I. Policies and Procedures: The CDRSN and, as applicable, its offices, programs and facilities must document the following actions relating to its policies and procedures:
- Required Policies and Procedures: The CDRSN and, as applicable, each office, program or facility of the CDRSN shall design and implement policies and procedures to assure appropriate safeguarding of PHI in its operations.
  - Changes to Policies and Procedures: The CDRSN, or an office, program or facility, must change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. The entity also may make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, the entity must make correlative changes in its Privacy Notice. The entity may not implement a change in policy or procedure prior to the effective date of the revised Privacy Notice.
- J. Documentation Requirements:  
The CDRSN must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the HIPAA regulations, for a period of six (6) years from the later of the date of creation or the last effective date.