

<b>CHELAN-DOUGLAS RSN/PIHP POLICY AND PROCEDURE MANUAL</b>		Chapter:	6.2.2.1
Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Page:	1 of 2
		Date Effective:	Nov. 1, 2003
Subject:	Acceptable Encryption	Date Revised:	Nov. 1, 2003 October 20, 2011
		Authorizing Signature:	

**AUTHORITY:** Authorizing Source: RCW 70.02 45 CFR 164 (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:** The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

**DEFINITIONS:** Proprietary Encryption: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

**POLICY:** Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Chelan-Douglas Regional Support Network's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Douglas County IT Director and Chelan-Douglas Regional Support Network Information Services Staff. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.