

CHELAN-DOUGLAS RSN/PIHP POLICY AND PROCEDURE MANUAL		Chapter:	6.2.2.9
Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Page:	1 of 2
		Date Effective:	Nov. 1, 2003
Subject:	Automatically Forwarded Email	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: This document explains Chelan-Douglas Regional Support Network recommended processes to prevent the unauthorized or inadvertent disclosure of sensitive company information.

DEFINITIONS: Email: The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.

Forwarded email: Email resent from internal networking to an outside point.

Sensitive information: Information is considered sensitive if it can be damaging to Chelan-Douglas Regional Support Network or its customers' dollar value, reputation, or market standing.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

POLICY: This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Chelan-Douglas Regional Support Network.

Employees must exercise utmost caution when sending any email from inside Chelan-Douglas Regional Support Network to an outside network. Unless approved by Chelan-Douglas Regional Support Network Privacy Officer, Chelan-Douglas Regional Support Network email will not be automatically forwarded to an external destination. Sensitive information, as defined in the Information Sensitivity Policy,

will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the Acceptable Encryption Policy.

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