

CHELAN-DOUGLAS RSN/PIHP POLICY AND PROCEDURE MANUAL		Chapter:	6.2.2.30
Title:	HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT	Page:	1 of 5
		Date Effective:	April 14, 2003
Subject:	Workstation Acceptable Use	Date Revised:	April 14, 2003
		Date Revised:	June 9, 2011
		Authorizing Signature:	

AUTHORITY: Authorizing Source: RCW 70.02.150; 45 CFR 164.310

SCOPE: This policy applies to Chelan-Douglas Regional Support Network/Prepaid Inpatient Health Plan (Chelan-Douglas RSN/PIHP) and its contractors (agencies/providers), subcontractors (referred to as contractors or agencies or providers throughout this policy) and Business Associates who have been granted logon rights to the Chelan-Douglas RSN/PIHP internal network.

PURPOSE: The purpose of this policy is to outline the acceptable use of computer equipment at the Chelan-Douglas RSN/PIHP. These rules are in place to protect the employee and Chelan-Douglas RSN/PIHP. Inappropriate use exposes Chelan-Douglas RSN/PIHP to risks including virus attacks, compromise of network systems and services, and legal issues.

POLICY:

I. General Use and Ownership

1. While the Chelan-Douglas RSN/PIHP desires to provide a reasonable level of privacy, users should be aware that any data created on Chelan-Douglas RSN/PIHP systems are the property of the Chelan-Douglas RSN/PIHP. Because of the need to protect the Chelan-Douglas RSN/PIHP network, management cannot guarantee the confidentiality of user information stored on any network device belonging to the Chelan-Douglas RSN/PIHP.
2. Employees are responsible for exercising good judgment regarding the reasonableness of computer use. If there is any uncertainty, employees should consult their supervisor.
3. IS staff recommends that any information that users consider sensitive or vulnerable be encrypted or stored in a folder requiring user authentication for access.
4. For security and network maintenance purposes, authorized individuals within the Chelan-Douglas RSN/PIHP and/or the Douglas County IT department may monitor equipment, systems and network traffic at any time.

5. The Chelan-Douglas RSN/PIHP reserves the right to audit networks and systems, including file and folder access logs, on a periodic basis to ensure compliance with this policy.

II. Security and Proprietary Information

1. Protected Health Information is maintained on Chelan-Douglas RSN/PIHP local resources in a manner that requires authorization for access in accordance with the Information Systems Security Policy & Procedure (1.4.2.25). Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
3. All workstations and laptops are configured with a password-protected screensaver with the automatic activation feature set to at 15 minutes, or by logging-off when the host will be unattended.
4. Use encryption of information in compliance with the Chelan-Douglas RSN/PIHP Acceptable Encryption Policy (6.2.2.1).
5. All workstations or laptops used by the employee that are connected to the Chelan-Douglas RSN/PIHP network shall be continually executing approved virus scanning software with a current virus database.
6. Employees must use extreme caution when clicking on links in e-mail messages or opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs or Trojan horse code.

III. Unacceptable Use

1. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities.
 - (a) Under no circumstance is an employee of the Chelan-Douglas RSN/PIHP to engage in any activity that is illegal under local, State, Federal or international law while utilizing Chelan-Douglas RSN/PIHP-owned resources;
 - (b) Violations of the rights of any person or company protected by copyright, trade secret, patent or any other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not licensed for use by the Chelan-Douglas RSN/PIHP.
 - (c) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrights sources, copyrighted music, and the installation of any copyrighted software for which the Chelan-Douglas RSN-PIHP does not have an active license is strictly prohibited.
 - (d) Exporting software, technical information, encryption software or technology, in violation of international or regional export laws, is illegal. Chelan-Douglas RSN/PIHP IS department or Douglas

County IT department staff should be consulted prior to export of any information that is in question.

- (e) Introduction of malicious programs onto the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.)
- (f) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
 - (i) The only exception to this is when IS/IT staff needs to temporarily elevate user privileges for the purpose of installing profile-specific software.
 - (ii) This exception is only specific to the use of your account by another. You shall never reveal your account password. IS/IT staff will temporarily reassign your password and, when work is complete, will reset your password so that you may maintain password secrecy.
- (g) Using a Chelan-Douglas RSN/PIHP IS/IT asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- (h) Making fraudulent offers of products, items or services originating from any Chelan-Douglas RSN/PIHP account.
- (i) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- (j) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to:
 - (i) Accessing data of which the employee is not an intended recipient or is not otherwise authorized to access.
 - (ii) Logging into a server or account that the employee is not expressly authorized to access.
 - (iii) For the purpose of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- (k) Port scanning or security scanning is expressly prohibited except as required to conduct scheduled network vulnerability analyses.
- (l) Executing any form of network monitoring which will intercept data not intended for employee's host, unless this activity is part of the employee's normal job duties.
- (m) Circumventing user authentication or security of any host, network or account.
- (n) Interfering with or denying service to any user other than the employee's host.
- (o) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the internet/intranet.
- (p) Connecting any non-Chelan-Douglas RSN/PIHP peripherals (keyboards, modems, printers, etc.).

- (q) Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
- (r) Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
- (s) Unauthorized use, or forging, of e-mail header information.
- (t) Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- (u) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- (v) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

IV. Workstation/Laptop Computer Use

- (1) Employees, contractors and others using portable computers (users) must read, understand and comply with this policy.
 - (a) Computers, associated equipment, and software are for business use only, not for personal use or the user or any other person or entity.
 - (b) Users will not download any software onto the computer except as loaded by authorized staff.
 - (c) Users are responsible for securing portable computer equipment within their homes, cars or other locations in the event the said equipment is removed from Chelan-Douglas RSN/PIHP facilities.
 - (d) Users may not leave mobile computer equipment unattended unless they are in a secure location.
 - (e) Users should not leave mobile computer equipment in cars or car trunks for an extended period in extreme weather (hot or cold) or leave them exposed to direct sunlight.
 - (f) Users must securely place portable computers and associated equipment in their proper carrying cases when transporting them.
 - (g) Users must not alter the serial numbers and asset numbers of the equipment in any way.
 - (h) Users will not allow anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, clients, client families, or unauthorized officers, employees and agents of the Chelan-Douglas RSN/PIHP.
 - (i) Users must not share their passwords with any other person and must safeguard their passwords and may not write them down so that an unauthorized person can obtain them (see Information Systems Security Policy & Procedure).
 - (j) Users must report in writing any breach of password security immediately to the Security Officer.
 - (k) Protected Health Information may not be stored on any portable computer or device, including laptops, flash drives, compact discs, diskettes, portable hard drives or other form of electronic data

storage that is not a component of the local network (see Information Systems Security Policy & Procedure).

- (l) Users must maintain confidentiality when using computers. The screen must be protected from viewing by unauthorized personnel when confidential information is displayed, and users must properly log out of the computer when it is not in use.
- (m) Users must immediately report any lost, damaged, malfunctioning, or stolen equipment or any breaches of security or confidentiality to the Security Officer.

V. Enforcement

- (1) Chelan-Douglas RSN/PIHP management is responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment.