



## PENINSULA RSN

### HIPAA AND MEDICAID COMPLIANCE POLICIES AND PROCEDURES

**Policy Name:** HIPAA E-MAIL AND INTERNET SECURITY  
POLICY

**Policy Number:** 5.12

**Reference:** 45 CFR Parts 160, 162 and 164;  
Kitsap County Electronic Communication Policy

**Effective Date:** 5/2005

**Revision Date(s):** 1/2008

**Approved by:** PRSN Executive Board

#### CROSS REFERENCES

- Policy: Password Protection Procedure, HIPAA
- Policy: Corrective Action Plan

#### PURPOSE

##### Introduction

The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that these policies be established, enforced, and audited. Peninsula Regional Support Network (PRSN) uses these and other policies to set limits on the use of email, PCs, cell phones, and telecommunications by employees.

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) on personal computers and servers.

##### Scope

The policies apply to PRSN employees and business associates, and covers e-mail located on PRSN computers if these systems are under the jurisdiction and/or ownership of PRSN. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

## PROCEDURE

### 1. Company Property

As a productivity enhancement tool, PRSN encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of PRSN and are not the property of users of the electronic communications services.

### 2. User Separation

These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. But, fax machines that do not have separate mailboxes for different recipients need not support such user separation. All PRSN staff and authorized business associates have unique usernames and passwords to access the e-mail system.

### 3. User Accountability

- a. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password, and it exposes PRSN to considerable risk.
- b. If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess - not a dictionary word, not a personal detail, and not a reflection of work activities. (Reference the HIPAA Password Protection Procedure.)

### 4. No Default Protection

Employees are reminded that PRSN electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. Consult the IS Manager if this requirement is needed.

### 5. Respecting Privacy Rights

- a. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. PRSN is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, PRSN also is responsible for servicing and protecting its electronic communications networks.

To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

- b. It is the policy of the PRSN that no e-mail message shall be sent or received that contain protected health information (PHI). If at any time either a PRSN employee or contractor use e-mail to transmit PHI as part of an e-mail message, the PRSN employee shall notify the sending party that e-mail is not to be used for this purpose; delete the message from their mailbox; and empty their e-mail trash.
- c. All electronic communications containing PHI shall be protected and secure as defined by this policy, and may be accomplished by accessing the shared network drive through the system Virtual Private Network/Secure Socket Layer system.

#### 6. No Guaranteed Message Privacy

PRSN cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

#### 7. Regular Message Monitoring

It is the policy of PRSN **NOT** to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored to support operational, maintenance, auditing, security, and investigative activities. PRSN retains the right to monitor messages to ensure compliance with HIPAA regulations concerning security and client privacy. Users should structure their electronic communications in recognition of the fact that PRSN will from time to time examine the content of electronic communications.

#### 8. Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. PRSN sensitive information must not be forwarded to any party outside PRSN without the prior approval of their manager.

#### Responsibilities

As defined below, PRSN staff responsible for electronic mail security has been designated in order to establish a clear line of authority and responsibility.

- Information Systems must establish e-mail security policies and standards and provide technical guidance on e-mail security to all PRSN staff.
- The Privacy Officer must review all such policies and procedures to ensure compliance with the agency's overall Privacy and Security Plan and to ensure compliance with applicable HIPAA regulations.

- IS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the personal computer security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
- PRSN managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.

9. Contact point

Questions about this policy may be directed to the Privacy Officer.

10. Enforcement

Violation of these policies may subject employees or business associates to disciplinary procedures in accordance with Kitsap County's personnel policies.

## **MONITORING**

This policy is mandated by contract or statute.

1. This policy will be monitored through use of PRSN:
  - Annual PRSN Provider and Subcontractor Administrative Review
2. If a provider performs below expected standards during the review listed above, a Corrective Action will be required for PRSN approval. Reference PRSN Corrective Action Plan Policy.