



| | | | |
|---------------|--|-----------------|---------|
| Subject: | E-mail Security & Acceptable Use Policy | Policy No: | TS108 |
| Signature | | Original Issue: | 4/12/05 |
| SEC Approval: | Marilee McGuire | Date: | 4/12/05 |
| Prepared By: | Jeff Cains | Effective Date: | 4/20/05 |

Purpose:

The purpose of this policy is to protect the confidentiality and integrity of sensitive information such as electronic protected health information (ePHI) that may be sent or received via e-mail. Further, the purpose is to provide an acceptable e-mail usage standard for employees of Community Health Plan (CHP).

Scope:

This policy applies to all CHP workforce members including, but not limited to full-time employees, part-time employees, contractors, temporary workers, trainees, volunteers, and anyone else granted access to sensitive information by CHP. Further, the policy applies to all systems, computer network, and applications, as well as all facilities, which process, store or transmit ePHI.

Policy:

E-mail Security

CHP recognizes that using e-mail without the use of an encryption mechanism is an insecure means of sending and receiving messages. CHP will evaluate emerging encryption solutions for e-mail and implement better solutions as they are found to be:

- Technically sound
- Reasonable to implement and use by workforce members
- Financially reasonable

The CHP provided e-mail systems are intended for official and authorized purposes only. E-mail messages are considered company property. Therefore, e-mail equipment operated by or for CHP staff is subject to the same restrictions on their use as any other company furnished resource provided for use by members of the workforce.

Electronic information about an individual, i.e. employer or member, in an organized set of records should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.

E-mail system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by the appropriate CHP Human Resources Executive and the Security Officer. However, CHP will have access to e-mail messages whenever there is a legitimate purpose for such access, i.e. technical or administrative problems.

Acceptable Use Policy

- While CHP's desires to provide a reasonable level of privacy, users should be aware that the data they create on company computer networks remains the property of CHP, including e-mail messages whether sent or received.

- Because of the need to protect CHP's computer networks, the confidentiality of information stored on any network device belonging to users cannot be guaranteed.
- CHP reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- The e-mail system is to be used mainly for CHP business use. However, some personal use of CHP's e-mail system is allowable provided that:
 - Both quality of the user's work and the user's production of work is kept at an acceptably high level.
 - The e-mail system is not used to send or receive messages or attachments that discriminate against or degrade a group or individual based on gender, sexual orientation, marital status, age, disability, race, nationality, religion, creed, or any other status that is protected by local, state or federal law.
 - Electronic mail is not used to inappropriately, illegally or unethically share CHP information, which is confidential, copyright protected, a trade secret, proprietary in nature or financial.
 - The e-mail system is not used to solicit or advertise non-CHP business ventures, advance a political cause or for religious proselytizing.

Responsibilities:

All individuals identified in the scope of this policy are responsible for abiding by the terms and guidelines set forth by this policy

The CHP Security Officer is responsible for:

- Evaluating on a periodic basis emerging encryption solutions for e-mail and implementing better solution when one is found that meets the criteria described in the policy section of this document
- Maintaining procedures and forms in support of this policy
- Monitoring and enforcing workforce compliance with this policy

Compliance:

Failure to comply with this or any other security policy will result in disciplinary actions as described in the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Procedure(s):

Before sending ePHI via e-mail outside of CHP to an e-mail address not ending with "chpw.org" users shall do the following:

1. Place and save the ePHI content in a separate document file, such as Word or Excel.
2. Right-click on the saved file to add the content to WinZip 9.0.
3. Within the newly created WinZip file click password and select a strong password to encrypt the file. A password is considered strong when the following is true:
 - The password is at least eight characters long and contains characters from each of the following three groups:
 - Uppercase and lowercase letters
 - Numbers
 - Symbols - character that are not define as letters or numerals (i.e. ~`@#%\$^&*()_+={[]:;'"<>./?)
 - And the password must**
 - Be significantly different from prior passwords
 - Not contain your name or user name
 - Not be a common word or name
4. Attached the encrypted WinZip 9.0 file to an e-mail message created in Microsoft Outlook and send it to the recipient.
5. Call the recipient to provide them with the password

Locking Computer Access

When e-mail or workstations are not in use, and a user is away from their desk, the user is to lock access to their computer to prevent unauthorized access. Users may lock access to their computers by password protecting the screen savers or manually hold down the Ctrl, Alt and Del keys on the keyboard and selecting Lock Computer from the dialogue box.

E-mail Disclaimer

The following disclaimer shall be placed at the bottom of E-mail messages:

“This message is intended for the sole use of the individual and entity to whom it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended addressee, nor authorized to receive for the intended addressee, you are hereby notified that you may not use, copy, disclose or distribute to anyone the message or any information contained in the message. If you have received this message in error, please immediately advise the sender by reply email and delete this message. Thank you very much.”

Form(s):

None

Definition(s):

Definitions for all policies are included in the glossary section of the Appendix.

References:

- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.
- Getting Started with HIPAA, Uday O. Ali Pabrai, Premier Press, April 2003.
- CMS, “CMS Information Systems Security Policy, Standards and Guidelines Handbook”, CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E))

Contact:

See Master Contacts List

| Revision History | | |
|------------------|---|------------------|
| Revision Date | Revision | Revision Made By |
| 10/24/05 | Removal of Contacts and consolidation in Master Contact List | Carrie Hardie |
| 3/22/06 | Changed all references from “Community Health Plan” to “Community Health Plan” and “CHP” to “CHP” | Carrie Hardie |