COPPER COUNTRY MENTAL HEALTH SERVICES BOARD

POLICY AND PROCEDURE

DATE: April 24, 2019 E-Mail Usage.P2

RESCINDS: May 29, 2013

CATEGORY: Administration

SUBJECT: E-mail Usage

POLICY: It is the policy of Copper Country Mental Health Services Board (CCMHS) to provide to authorized staff, access to Agency e-mail facilities.

PURPOSE: To define access and use of the resource and establish guidelines for the appropriate use.

PROCEDURE:

Electronic mail (e-mail) is defined as the exchange or storage of electronic messages and files between computers that are connected to the CCMHS' network or the Internet.

I. Appropriate Use of Electronic Mail (E-Mail):

A. Individuals at CCMHS are encouraged to use e-mail to further the goals and objectives of CCMHS. The types of activities that are encouraged include:

1. Common communication with fellow employees and business partners within the context of an individual's assigned responsibilities
2. Non-treatment related communication with groups that work with persons served (e.g. NAMI, the Consumer Advisory Committee, etc.)
3. Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities
4. Participating in educational or professional development activities

B. Official CCMHS' communications may be delivered via the e-mail system. Employees with e-mail accounts are expected to check their e-mail in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks.

C. E-mail users are responsible for mailbox management, including organization and cleaning.

D. E-mail access will be terminated when the employee leaves employment with CCMHS. CCMHS is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of their employment has ceased.

E. It is the responsibility of the employee to protect the confidentiality of their account and password information.

F. Extreme caution shall be used when communicating via e-mail. E-mail messages sent outside of CCMHS becomes the property of the receiver. Do not communicate anything that you wouldn't feel comfortable being made public.

II. Sending or Receiving E-Mails Containing ePHI:

A. Receiving unsolicited e-mail messages from persons served, or their parents or guardians, containing ePHI shall be forwarded to the Records Department to be added to the record of the person served.

1. The recipient of the e-mail, if not the Primary clinician of the person served, shall notify the appropriate clinician of the incident.

a) The Primary clinician shall discuss the inappropriateness of the e-mail communication with the sender via telephone or face-to-face conversation.

2. If the recipient of the e-mail is the Primary clinician of the person served, he or she shall discuss the inappropriateness of the communication.

B. E-mail is not considered a completely secure form of communication. Therefore, unencrypted ePHI sent to non-CCMHS e-mail accounts is not permitted.

1. E-mail encryption shall be utilized for e-mails containing ePHI sent outside the CCMHS' e-mail system.

2. Additional e-mail security and encryption training is required for all employees prior to initial e-mail communication. The employee shall request this training from the HIPAA Security Officer.

C. E-mail communication between CCMHS staff members and a person served, or their parent or guardian is not permitted

without a signed consent form.

D. Messages containing ePHI should be avoided. If required, provide only the minimally necessary information to the receiving party including only initials and MCO number on e-mail.

E. All professional and medical records requirements shall be adhered to. This may include, but is not limited to, one or more of the following: "need to know", confirming a release of information and documentation in the clinical chart.

III. Inappropriate Use of E-Mail:

A. Use of e-mail in any way that violates CCMHS' policies or rules.

B. Use of e-mail for illegal or unlawful purposes includes but is not limited to: Copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).

C. Inappropriate use of e-mail including but is not limited to: unsolicited mass mailings, non-CCMHS' commercial activity, political campaigning, dissemination of chain letters, and use by non-CCMHS' employees.

D. CCMHS' e-mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems, cause a breach of the confidentiality of persons served or divulge sensitive financial information.

E. Viewing, copying, altering, or deleting of e-mail accounts or files belonging to CCMHS or another individual without authorized permission.

1. Storing large files in a Lotus Notes forum and sending only a link to the forum entry is the preferred method to disseminate large files to CCMHS' employees.

F. Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with the utmost caution.

G. Sharing e-mail access with another person or attempting to obtain another person's e-mail account password. E-mail accounts are only to be used by the registered user.

H. Excessive personal use of CCMHS' e-mail resources. CCMHS allows limited personal use for communication with family and friends, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources.

I. Independent learning and continuing education is permitted with approval from the employee's supervisor. The learning should not interfere with regular job responsibilities or productivity.

J. The use of personal email addresses for CCMHS business is prohibited unless approved in advance by the IT Department (this includes non-authorized email domains such as gmail.com, etc.).

IV. E-Mail Account Administration:

A. The e-mail systems and services are owned or operated by CCMHS, and therefore, Agency property. This gives CCMHS the right to monitor any and all e-mail traffic passing through its e-mail systems and/or communication networks.

B. Personal or business e-mail messages residing in CCMHS' e-mail system is the property of CCMHS. Access may be revoked at any time.

C. Despite end-user deletion, backup copies of e-mail messages may exist in compliance with CCMHS' disaster recovery procedures. The goals of these backup and archiving procedures are to ensure system reliability, provide evidence for investigations and prevent business data loss.

D. If it is discovered or there is reason to suspect activities that do not comply with applicable laws or Agency policies or procedures, e-mail records may be retrieved and used to document the activity in accordance with due process outlined in the CCMHS' Corrective/Progressive Discipline Policy.

V. Reporting Misuse:

A. Any allegations of misuse shall be promptly reported to the HIPAA Security Officer.

B. If you receive an offensive e-mail, do not forward, delete or reply to the message. Instead, report it directly to the HIPAA Security Officer.

VI. Sanctions for Misuse:

A. Sanctions for inappropriate use of e-mail may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of access to some or all computing, networking or communication resources and facilities

2. Disciplinary action according to the CCMHS' Personnel Policy

3. Legal action according to applicable laws and contractual agreements

APPLICATION: This procedure applies to all staff members and includes all e-mail systems and services operated by CCMHS, all e-mail account users/holders (both temporary and permanent), and all e-mail records.

The Director of Information Technology is responsible for monitoring this procedure.

CROSS REFERENCE:

CCMHS Policy - Information Management and Access Control

CCMHS Policy - Workstation Usage and Security

CCMHS Policy - Internet Usage

All CCMHS' policies pertaining to our electronic infrastructure under Administration policies found under Section 2 pages 38 through 167.