SOUTHERN HIGHLANDS COMMUNITY MENTAL HEALTH CENTER

POLICY AND PROCEDURE MANUAL

Date of Issue: 8/6/02 **Section Number 243**
Date Revised: 4/7/05; 7/21/09; 1/1/15; 3/24/16; 6/24/20

Policy 243 – E-Mail Policy

I. POLICY

The purpose of this policy is to ensure the proper use of Southern Highlands' e-mail system and make users aware of what SHCMHC deems as acceptable and unacceptable use of the electronic mail (e-mail) system. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that e-mail policies be established, enforced and audited.

II. PURPOSE

The purpose of this policy is to define proper use of SCHMHC's e-mail on any electronic device. By using these systems, employees agree to comply with this policy. This policy statement provides specific instructions on the ways to secure e-mail on personal computers and servers.

This policy applies to any electronic devices which are capable to send and receive email, including, but not limited to, desktops, thin clients, laptops, iPads, tablets**,** and cell phones.

III. LEGAL RISKS

E-mail is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature e-mail seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail.

- If you send or forward e-mail with any libelous, defamatory, offensive, racist or obscene remarks, you and SHCMHC can be held liable.
- If you unlawfully forward confidential information, including consumer private health information, you and SHCMHC can be held liable.
- If you unlawfully forward or copy messages without permission, you and SHCMHC can be held liable for copyright infringement.
- If you send an e-mail that contains a potentially harmful attachment, such as a virus, malware, etc., you and SHCMHC can be held liable.

By following the guidelines in this policy, the e-mail user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set forth in this E-mail Policy, the user will be fully liable and SHCMHC will disassociate itself from the user as far as legally possible.

IV. LEGAL REQUIREMENTS

The following rules are required by law and are to be strictly adhered to.

- If you have Center e-mail on a mobile device, the device **must have a password to unlock.** (If your mobile device is not password protected, contact the IT Department to set up password protection before using it for SHCMHC e-mail.)

It is prohibited to:

- Send or forward e-mails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.
- Forward a message without acquiring permission from the sender first.
- Forge or send unsolicited e-mail messages.
- Forge or attempt to forge e-mail message.
- Disguise or attempt to disguise your identity when sending mail.
- Send e-mail messages using another person's e-mail account.
- Copy a message or attachment belonging to another user without permission of the originator.

V. BEST PRACTICES

SHCMHC considers e-mail (to include Microsoft Teams) as an important means of communication and recognizes the importance of proper e-mail content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an e-mail as they would for any other communication. Therefore, SHCMHC e-mail users must adhere to the following guidelines.

A. Writing e-mail

1. Write well-structured e-mails and use short, descriptive subjects.
2. SHCMHC's e-mail style is informal. This means that sentences can be short and to the point. The use of Internet abbreviations and characters such as smileys, however, is not encouraged.
3. Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature (see disclaimer).
4. Users must spell check all e-mails prior to transmission.
5. Do not send unnecessary attachments. Compress all e-mail attachments.
6. Do not write e-mails in capital letters.
7. Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying an e-mail to him/her and knows what action, if any, to take.

8. Recognize that some information is intended for specific individuals and may not be appropriate for general distribution. Electronic communication users should exercise caution when forwarding messages. E-mail replies should delete originally sent PHI. E-mails should not use consumer names or other identifiers as the subject of the message.

9. Only send e-mails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the e-mail, using other means of communication, or protecting information through encryption.

10. Only mark e-mails as important if they really are important.

11. SHCMHC's antivirus software is configured to automatically scan email attachments, however, this does not guarantee that an attachment is safe to open. Exercise caution when opening email attachments. If you receive an unsolicited attachment or if an attachment appears to be suspicious contact the IT Department.

B. Newsgroups

Users need to request permission from their supervisor before subscribing to a newsletter or news group. If the source of the newsletter or news group is unknown or questionable, the supervisor must obtain approval from the IT Department.

C. Maintenance

The amount of space your e-mail consumes on the e-mail server is finite. Delete any unwanted/needed e-mails in a timely manner in order to keep your inbox clutter free to improve e-mail performance..

Any e-mail you feel that is needed to be kept for the long-term, copy to your fileserver share ("Z:/" or otherwise known as "My Documents"). If you are unsure of how to do this, contact the IT Department.

VI. AUTHORIZED USAGE

SHCMHC's e-mail system must be used only for Southern Highlands business activities. Use of the SHCMHC e-mail system for personal use is prohibited and must be reported to the individual's supervisor or the IT Department.

Forwarding of e-mails not pertaining to work related activities is prohibited. If you receive an e-mail from a fellow SHCMHC employee that is of this nature, (i.e., joke, chain mail, etc) please delete the e-mail from you inbox immediately.

MOBILE E-MAIL: If you have a cell phone with "data plan" you may be able to receive your Southern Highlands e-mail on your device. The ONLY means of obtaining e-mail on your mobile device is by means of Internet Message Access Protocol 4 (IMAP/4) and should be set up by an IT staff person. DO NOT attempt to connect to the SHCMHC.COM domain on your mobile device without contacting the IT Department first. All mobile devices with Southern Highlands e-mails must be locked with a password.

VII. CONFIDENTIAL INFORMATION

SHCMHC will treat all e-mail messages sent or received that concern the consumer as part of the consumer's medical record and treat it with the same degree of confidentiality as other parts of the record. All emails sent through SHCMHC server are secure. Any email being sent outside of the SHCMHC, staff must note "secure" in the subject line of the email.

All e-mail concerning consumer information must contain the confidentiality disclaimer below.

"This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error, please notify sender and may not read, copy, or distribute this e-mail. Please note that any views or opinions presented in the e-mail are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this e-mail."

VIII. PASSWORDS

Regardless of the circumstances, individual passwords must never be shared or revealed to anyone, including IT staff. Should the IT Department need access to a user's e-mail account the user will be required to perform the log in. Baring this, the network administrator may override the user's passwords and require it to be changed on the user's next login. Email passwords will be changed every 90 days. The system will automatically notify the user that the email password is needing to be changed as outlined in Password Policy (Policy 244).

IX. E-MAIL RETENTION

All e-mail that is sent or received on the "SHCMHC.COM" domain is archived for a minimum of seven years as required by law. If an e-mail has been accidentally deleted, it may be possible to be restored by contacting someone in the IT Department. Not all e-mails are recoverable.

Please keep your inbox and other mail folders clutter free. E-mail should NOT be stored indefinitely within your e-mail inbox, but rather important e-mail messages should be stored within your fileserver share (otherwise known as Z:/ or "My Documents"). The clinical staff will decide standards for determining whether a particular e-mail message will constitute part of a patient's medical record. Messages containing PHI should be scanned by the Medical Records Department and then the e-mail must be deleted or be stored in a secure electronic folder (i.e., Z:/ or "My Documents"). It is always a good rule to password protect sensitive data files. If you are unaware of the procedure of password protecting a file, please call the IT Department.

X. E-MAIL ACCOUNTS

All e-mail accounts maintained on our e-mail system are property of SHCMHC. The e-mail system and all messages generated by or handled by e-mail, including back-up copies, are part of the business equipment of SHCMHC, are owned by SHCMHC, and are not the property of the users of the system. If an employee resigns from their position or is terminated, the email account will be disabled. Some email accounts may be disabled if an employee is on administrative leave pending an investigation. Staff that are on leave or have left the agency may have emails sent to direct supervisor.

XI. SYSTEM MONITORING

Users expressly waive any right of privacy in anything they create, store or receive on SHCMHC's computer system. SHCMHC will monitor e-mails without prior notification to ensure compliance with HIPAA regulations concerning security and consumer privacy. Users should structure their e-mail in recognition of the fact that SHCMHC may from time to time examine the content of their e-mail. If there is evidence that you are not adhering to the guidelines set out in this policy, SHCMHC reserves the right to take disciplinary action, including termination and/or legal action.

It may be necessary for IT staff to review the content of an individual employee's communications during the course of problem resolution.

If a user receives an email they feel is corrupt or unusual, the user will contact IT department to review the email. Users are prohibited from opening attachments from unknown senders or attachments that seem unusual.

XII. RESPONSIBILITIES

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

A. Information Technology must establish e-mail security policies and standards and provide technical guidance on e-mail security to all SHCMHC staff.

B. The Privacy Officer and the Security Officer will review all e-mail policies and procedures to ensure compliance with the agency's overall Privacy and Security Plan and to ensure compliance with applicable HIPAA regulations.

C. IT staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. IT staff must also provide administrative support and technical guidance to management on matters related to e-mail security.

D. SHCMHC supervisors will ensure that employees under their supervision implement e-mail security measures as defined in this document.

E. Users must immediately report violations of this policy to their department heads and to the Security Officer.

XIII. DISCLAIMER

The following disclaimer will be added to each outgoing e-mail:

"This e-mail and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error, please notify sender and may not read, copy, or distribute this e-mail. Please note that any views or opinions presented in the e-mail are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this e-mail and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this e-mail."

XIV. QUESTION

If you have any questions or comments about this E-mail Policy, please contact the Security Officer. If you do not have any questions, SHCMHC presumes that you understand and are aware of the rules and guidelines in this E-mail Policy and will adhere to them.

XV. DECLARATION

I have read, understand and acknowledge receipt of the E-mail Policy. I will comply with the guidelines set out in this policy and understand that failure to do so may result in disciplinary action, including potential termination of employment, or legal action.

Signature: ________________________________

Date: ____________________________________

Printed Name: _____________________________