SAN MATEO COUNTY HEALTH
BEHAVIORAL HEALTH & RECOVERY SERVICES

Policy:	**22-06**
Subject:	**Electronic Communications Policy (General Guidelines)**
Authority:	42 CFR Part 2, 2.16(a); 45 CFR Part 160; 45 C.F.R. Part 164, Subpart A, C, and E; San Mateo County E-Mail Policy; CA Code of Regulation Title 16 Section 1815.5: Standards of Practice for Telehealth; DHCS BHIN 22-019; DHCS BHIN 23-018.
Original Policy Date:	October 14, 2022
Amended:	Technical Edit September 4, 2024
Supersedes:	Cell Phone Usage: 01-01 Facsimile (FAX) Confidentiality: 01-07 Email Use: 03-11
Attachments:	Attachment A: De-identifying Protected Health Information Attachment B: Protocol for Email Usage Attachment C: Sending Secure Emails

PURPOSE

This policy is intended to establish general guidelines for the use of electronic communications by staff, with emphasis on the privacy and confidentiality of Protected Health Information (PHI). Electronic communications for the purposes of this policy include E-mail, SMS (text), computerized voice messaging, voice mail messages, fax communications, telehealth (videoconferencing) platforms, and automated messages (e.g., appointment reminders).

For guidelines on the proper use of electronic communications with clients, please review both this policy and BHRS Policy 22-07 Electronic Communication (Communication with Clients).

SCOPE

This policy applies to all San Mateo County Behavioral Health and Recovery Services staff.

DEFINITIONS

I. **Facsimile (FAX)** – messages sent through a facsimile (FAX) machine.

II. **Mobile Device** – Any portable electronic device used for communication. This includes cell phones, tablets, and laptops.

III. **Encrypted Communication** – When an electronic device or software is set up in a manner that prevents external parties from accessing the conversation. Example: Communication using the County's secure email platform or the County's Authorized Telehealth Platforms (Zoom Health and MS Teams) are encrypted, emails sent with "#sec#" in the subject line are encrypted.

IV. **Secure Communication** – This is another term for "encrypted" communication.

V. **Unencrypted Communication** – This form of communication is the least secure communication and is the easiest for external parties to access. Unencrypted communication does not have protections embedded into the programming to prevent external parties from accessing the communication. Emails sent without "#sec#" in the subject line and personal Zoom and MS Teams accounts are not encrypted.

POLICY

Any staff person engaging in electronic communication and/or electronic messaging for San Mateo County Behavioral Health and Recovery Services (BHRS) business is required to review and follow all relevant federal, state, and county policy, as well as the BHRS privacy and confidentiality policies available at the BHRS policy website: http://www.smchealth.org/behavioral-health-staff-forms-policies.

In addition, the following County-wide policies must also be adhered to:

- Mobile Technology Use Policy – San Mateo County Manager Administrative Memo B-19
- Information Technology Security Policy (ISD)
- Portable Computing Policy (ISD)

I. **Authorized Devices and Telehealth Platforms**

Staff may only use a password protected County-issued mobile device or BHRS authorized telehealth platform to call clients or other professionals, and as long as all required consents and/or Releases of Information are obtained.

A. **County Issued Cell Phones**

1. All staff are required to follow all County policies regarding safe cell phone usage while driving. (See County website.)
2. County issued mobile devices shall be available at all clinical sites and for all clinical teams that provide community-based services whenever possible. Managers or supervisors of individual sites/teams shall establish mobile device usage priorities and make this information available to all staff.
3. On occasion, an individual staff member may be assigned a County cell phone when it is established that cell phone usage, as defined in this policy, is an integral part of their routine work assignment.

a. Staff members typically assigned a County cell phone include those working in units with 24/7 on-call responsibilities and staff assigned to field-based or intensive in-home treatment programs.

b. The Unit Chief/Supervisor is responsible for recommending and assuring ongoing necessity for the specific assignment of a cell phone for the routine work needs of a staff member.

4. Cell phone usage is intended to provide immediate phone accessibility to a BHRS clinic, to PES or to 911 in the event of emergencies. Staff responding to a crisis call or potential 5150 situation in the community shall have priority for the use of a site cell phone.

5. Staff will turn off the phone during non-working time and keep it in a secure location. The outgoing voicemail greeting will give instructions for whom to contact in an emergency, both during and after hours, and state that this is a work phone and is only available during the employee's work schedule, which will be included in the voicemail message. This will be updated to reflect time away and state that the phone will be off during those times.

B. **Telehealth (videoconferencing) Platforms**

1. If conducting a video meeting with client(s) or to discuss client(s), staff should initiate the meeting using BHRS authorized telehealth platforms. Contact BHRS QM for the most up-to-date list of authorized platforms.

2. Staff may join meetings using another organization's telehealth platform if staff are able to confirm that the platform being used is HIPAA compliant.

3. If the telehealth platform being used is not confirmed to be HIPAA compliant, then staff may still attend the meeting, but should use caution when sharing information and avoid sharing sensitive information related to the client's treatment. Staff should not transmit documents via the non- HIPAA compliant platforms. If requested to send documents electronically through the non-HIPAA-compliant platform, staff should instead send the document through the County's secure email platform.

4. For additional guidelines related to meeting with clients over telehealth, see BHRS Policy 22-07 Electronic Communication (Communication with Clients).

II. Obtaining an Authorized Device or License to an Authorized Telehealth Platform

A. Obtaining a County Cell Phone

1. Read the required policies listed above
2. Obtain Supervisor or Manager Approval.
3. Follow BHRS protocols to submit a service ticket to request a mobile device and complete all required forms.
4. ISD will contact the user directly for issuance.

B. Obtaining a License to an Authorized Telehealth Platform

1. Read the required policies listed above.
2. Obtain Supervisor or Manager Approval.
3. Follow BHRS protocols to submit a service ticket to request the license.
4. BHRS IT will contact the user directly for issuance.

III. Unit Supervisor's Responsibility

Supervisors are responsible for educating their staff about appropriate mobile device use (e.g., cell phones) to ensure their understanding of the policies and to set the clear expectation that any concerns must be immediately brought to the supervisor's attention.

If inappropriate use of a mobile device occurs, the supervisor will ensure that an incident report is completed and turned into BHRS Quality Management (QM).

IV. Confidentiality Statements

Standard Confidentiality Statements should be included in all emails and faxes sent by staff.

A. Confidentiality Statement for Emails

All emails sent by staff that includes client information must include the following confidentiality statement:

Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message

B. **Confidentiality Statement for FAXes**

All FAX transmittals that contain client identifiers, sent from FAX machines located within Mental Health Services' provider sites, must include a cover sheet with the following confidentiality statement:

The information contained in this FAX transmission is confidential and may be privileged and exempt from disclosure under applicable law. This information is intended only for the use of the individual or entity to which it is addressed. If you are not the intended recipient, or the agent or the employee responsible to deliver it to the intended recipient, you are hereby notified that any use, dissemination, distribution, or copying of this communication is strictly prohibited. If you have received the FAX transmission in error, please immediately notify us by telephone and return the original message by mail to the address below (return postage available upon request). Thank you.

V. Checking Recipient Contact Information

A. It is the sender's responsibility to verify that the correct email address, phone/text number, or FAX number has been entered before transmitting any information. Best practice for phone numbers is to enter the entire seven-digit local number with the area code, rather than just the seven-digit number or the county four-digit number. For FAXes, whenever possible, locations receiving regular FAX transmissions should be entered into speed dialing options on the FAX machine (verify before initial use).

B. Extreme caution shall be observed when responding to "ALL" on a message. The responder must be certain of the entire mail list before deciding that PHI or other confidential material should be addressed to everyone who received the original message.

VI. Minimum Necessary

Staff should ensure that the amount of information included in the message is the minimum necessary to ensure that patient identifying information is non-identifiable and presents a very low risk of re-identification (e.g., removing direct identifiers such as first and last names). Additional information on de-identifying PHI is included in Attachment A of this policy.

1. An email to schedule a meeting regarding a client should only include a generic meeting title (does not include client name or other identifying information), the date/time of the meeting, and the URL or physical address of the meeting.

2. Client PHI should not be identified on the fax cover page or email subject line.
3. The use of Social Security numbers as the sole identifier does not adequately de- identify the client. Any communication using a Social Security number is still PHI.

VII. Secure Electronic Communication

Any disclosure of PHI should be done by phone from a private location or in-person, or through one of the BHRS approved, secure platforms with proper releases of information. Additional guidelines for communicating responsibly via an electronic format include:

A. Secure communication should be the default mode of electronic communication. Secure email should always be used when communicating with other professionals or providers. See Attachment C for instructions on sending secure messages.

   For details on protocols for sending unencrypted electronic communication (emails, texts, etc.) to clients, please follow guidelines in BHRS Policy 22-07 Electronic Communication (Communication with Clients).

B. All email sent within the County email system (emails ending with @smcgov.org) are secure. Any emails sent to or received from outside the County system is not secure.

   However, PHI should not be sent using a large email group (e.g., HS_BHRS_AllStaff) even if all email address in the group are within the County system.

C. Staff should not disclose PHI in any text message, including with County staff or any other colleagues. However, texting can be used to alert someone that there is an urgent situation that needs a discussion.

D. Staff should review with the recipient of the secure communication how to access the secure platforms (e.g., secure email platform).

E. It is not recommended that voicemail messages be forwarded to the cell phone.

VIII. Storage of Electronic Communications

A. Documents or messages that are of clinical significance should be scanned into the electronic medical record or paraphrased in a progress note. All hard copies of documents with client identifiers must be securely shredded when no longer needed.

B. Electronic communications of no clinical significance may be deleted when no longer needed.

IX. **Storage of Electronic Communication Devices**

A. Computers and FAX machines shall not be installed in areas where the public, including clients, may see or have access to material that has been sent or received.

B. All computers and mobile devices must be password protected and encrypted in accordance with San Mateo County security protocols.

C. Any county issued mobile device will be secured when not in use and each unit will establish a sign in/sign out procedure

Approved: *Signature on File*
Scott Gruendl, MPA
Assistant Director
Compliance Officer

Approved: *Signature on File*
Dr. Jei Africa, PsyD, FACHE
BHRS Director

ANNUAL REVIEW OF COMPLIANCE POLICY			
Next Review Due:	June 2025		
Last Reviewed by:	Scott Gruendl, Compliance Officer	**Date:**	6/18/24