Monterey County Behavioral Health
Policies and Procedures

Policy Number	Policy 496
Policy Title	Communication With Persons in Care
References	Code of Federal Regulations, Title 45, Section 160 and 164 42 CFR Part 2, California Health and Safety Code Sections 11942 et seq. Policy # 20-21 Protected Information Policy 149 Telehealth
Effective	10/1/2024

Policy

While providing services, it is appropriate for Monterey County Behavioral Health (MCBH) staff and its contracted providers to interact with persons in care using various forms of electronic communication. It is the intention of MCBH to ensure that its staff and contracted providers maintain professional boundaries for all types of electronic communication. MCBH's use of electronic communication methods is to be used as a business communication tool only. The systems and all messages they transport, or store are the property of MCBH. The purpose of this policy is to clarify the use of electronic communications with persons in care and to establish guidelines for its appropriate and secure use.

Procedure

The following procedures has been put in place for each form of electronic communication being used with persons in care. For any new and/or existing person in care, the staff shall review the potential limitations and risk and outline the expectations and responsibilities associated with these forms of communication and obtain signatures on the Electronic Communication Consent.

Email

I.   Email communication with a person in care must occur using the staff's county email, never their personal email account.
II. Any email communication with a person in care must take place using a county/provider-issued or approved device (i.e. laptop, cell phone).
III. Staff shall encrypt any and all emails containing PHI (include a person's PATID); if using an attachment, ensure this is also encrypted.
IV. Staff should double check that the person in care's email address is correct prior to sending.
V.   Email responses from the person in care shall be deleted after being read.

VI.   Staff must maintain professional business etiquette in all email communications with a person in care. Emails should begin with a salutation and end with your formal email signature and must include the standard confidentiality notice.

VII.   Email communication with a person in care should be limited to the minimum necessary content to successfully communicate needed information (logistical, obtaining documents, etc.); clinical or treatment information should be reserved for discussion in session.

VIII.   When staff are out of the office, an out of office automatic reply should be enabled, including information on how to seek support in the staff member's absence.

Telephone

I.   Telephone calls to a person in care should be made using either a county/provider desk phone or a county/provider issued cell phone. If it is unavoidable that a staff member must use their personal device to call a person in care, the staff member must block their number by pressing *67 or other blocking mechanisms prior to dialing.

II.   Staff should double check the phone number prior to calling the person in care.

III.   When contact is made with the person in care, staff should verify the location of the person and their current privacy before initiating sensitive conversation.

IV.   Staff should only leave voicemail if they are certain the phone number is correct.

V.   Voicemail messages left for the person in care should be kept as general as possible.

VI.   Staff's voicemail greeting should include crisis resources in the event of an urgent need. When staff are out of the office (vacation, leave, etc.), an out of office voicemail greeting should be recorded, including information on how to seek support in the staff member's absence.

Fax

I.   Staff should always double check the number is correct prior to sending a fax.

II.   A fax cover sheet with confidentiality statement prominently displayed shall be used any time a fax is sent.

III.   It is good practice to call the recipient to confirm a fax was received.

County/Provider-Approved Secure Text Messaging Platform

I.   Text messages to persons in care must be sent using a county/provider approved secure messaging platform. Staff should never share their personal phone number with persons in care, or text a person in care using their personal device.

II.   Staff should always confirm the person in care's number prior to sending a text message.

III.   Staff should maintain professional business etiquette when communicating with persons in care via text message.

IV.   Text messages should be limited to the minimum necessary information to convey the message. Clinical or treatment information should be reserved for

discussion in session. See "Appropriate Use of Email/Voicemail/Secured Text Message Communication" for more details.

<u>Consent</u>

Regardless of the specific method (i.e. email, fax, text messaging), consent must be obtained prior to engaging in any form of electronic communication with persons in care. At minimum, informed consent must include the following:

I. Monterey County does not assume any liability over the person in care's device(s).
II. The right of the person in care to opt out of receiving electronic communication and may consent or not consent to each individual form of electronic communication at will.
III. Appropriate, inappropriate, and prohibited use of electronic communication (see below).
IV. The limitations to privacy inherent to asynchronous communication, such as the possibility that others in the person in care's household might have access to the email, text, voicemail, etc.
V. The possibility that emails may be sent through an unsecured server, which could allow others to intercept and read the email message.
VI. Limitations on staff availability (e.g., staff will not answer calls or texts outside of work hours), and instructions on accessing after-hours or emergency care while staff are unavailable.

For specific notices and consent forms and details surrounding electronic communication, please see the Electronic Communication Consent Acknowledgement and 149 Telehealth Policy. In a progress note, the clinician shall document the discussion and person in care's consent for electronic communication, including if the person declines to sign the consent.

<u>Safeguards</u>

Safeguards are measures in place to protect data being shared electronically. Safeguards are applied across multiple levels from individuals to larger systems, to ensure confidentiality standards are upheld.

Administrative Safeguards

I. A staff member may utilize electronic communication with a person in care under the following conditions, which should be explained in detail at the onset of care, and reviewed as clinically indicated throughout the course of treatment:
   a. Person in care has been informed of the staff member's work hours and availability to respond to electronic communication as well as how to best obtain support in an emergency.
   b. Explicit consent for electronic communication must be obtained and documented (see "Consent" section above).
II. Once electronic communication is initiated, the staff member must confirm the person in care's contact information is accurate and up to date regularly.

Clinical Safeguards

I. Staff members shall use clinical judgment regarding the appropriateness of utilizing electronic communication methods with persons in care.

II. Staff members should limit mass or group secure text messages or emails to large groups of people, especially if any PHI is involved.

III. Secure text message, email, and voicemail should contain minimum information necessary, including PHI if applicable, to achieve the intent of the communication.

IV. Electronic communication exchanges must be documented within a progress note in accordance with the timeliness requirements in the Clinical Documentation Guide. Documentation of any asynchronous communication exchange (i.e., voicemail, secure text message, email) must meet the progress note requirements as outlined in Policy 23-068.

V. If there is no consent to text message/email and the person in care initiates the communication through these means, the staff member shall make other efforts to respond through another form of communication such as by telephone until consent is obtained.

VI. If the content of the person in care's message (via email/secure text/voicemail) indicates the presence of an urgent or emergency situation, the staff member shall respond to the person in care in the most expeditious and appropriate manner including through (when applicable) secure text message, regardless of whether a signed consent/agreement is on file. Staff shall keep in mind the safeguards mentioned above and make a clinical determination on how to best respond to the indicated 'urgent' or 'emergency' situation. Consultation with a supervisor and/or manager may be needed.

Technical Safeguards

I. Only authorized staff members who have county/provider-approved secure text messaging application installed on their device may send secure text messages.

II. Staff members shall refrain from installing the county/provider-approved secure text messaging application on unapproved devices.

III. All devices utilizing the county/provider-approved secure text messaging application must be password protected to prevent unauthorized access to confidential messages sent to or from the device, should the device become lost, misplaced, or stolen.

IV. Staff members must ensure that county/provider-approved secure text messaging application's secure Personal Identification Number (PIN) or password feature is enabled as an additional security safeguard for preventing unauthorized access to the confidential communication within the application.

V. Staff members are prohibited from using their device's built-in SMS, Apple iMessage, or any other third-party messaging application for communicating confidential data.

VI. Staff members must utilize call blocking to protect their device's identity and number, should they need to call a person in care from their personal device.

VII. If a staff member receives a text or video chat message that includes sensitive or

confidential information via an unsecure method such as the device's built-in SMS, Apple iMessage, or any other third-party messaging application, staff must respond to the sender via other means of communication (e.g., telephone) and delete the message immediately.

VIII. Saving or sharing text messages, pictures, and audio or video recordings outside of county/provider-approved secure text messaging application or other secure storage sites is strictly prohibited.

IX. When staff members register within the county/provider-approved secure text messaging application, they must accurately input and/or update their profile information within the application to ensure integrity and verification of parties involved.

X. Staff members are advised to take notes, and if applicable, ensure the communicated materials are documented in the clinical record in accordance with the timeframes described in the Clinical Documentation Guide.

Appropriate Use of Electronic Communication

Email/Voicemail/Text Communication

I. **Scheduling logistics:** this includes but is not limited to gathering information regarding person in care's availability for appointments, arranging appointments, and confirming appointments.

II. **Notifications or reminders**: this includes but is not limited to notifications about upcoming appointments or groups, links to material for persons in care to review or complete, and reminders such as completing lab work in preparation for a scheduled appointment.

III. **Treatment updates and/or person in care needs**: this information should be limited and clinical or treatment information should be reserved for discussion in session and/or through secure telecommunication methods.

Telephone (excluding voicemail) Communication

I. **Individual contacts**: this may include (but is not limited to) case management, individual therapy, mental health rehabilitation, medication support services, collateral with a support person, and "check-ins" between appointments.

II. **Group contacts**: this may include family or collateral encounters with multiple support persons present, group counseling, group therapy, and support team meetings between persons in care and varied members of their professional and natural supports.

III. **Scheduling logistics:** this includes but is not limited to gathering information regarding person in care's availability for appointments, arranging appointments, and confirming appointments.

IV. **Notifications or reminders**: this includes but is not limited to notifications about upcoming appointments or groups, links to or information about material for persons in care to review or complete, and reminders to complete lab work in preparation for a scheduled appointment.

Inappropriate Use of Electronic Communication

I. If a person in care sends treatment information, clinical information, or PHI to staff via email or text message, staff should reach out to the person in care by phone to follow up and schedule an appointment if needed. Staff shall remind the person in care (and/or their authorized representative) about the appropriate uses of electronic communication.

II. If a person in care shares inappropriate or explicit material with staff electronically, staff should immediately notify their supervisor, and an incident report should be completed and submitted to QI. Staff shall create a plan that addresses the inappropriate use of electronic communication in collaboration with the person in care (and/or their authorized representative) and the treatment team members.

III. Staff should consult with their supervisor in the event of any uncertainty around appropriateness of electronic communication with persons in care.

Prohibited Use of Electronic Communication

I. **PHI**: Sharing of any PHI (Protected Health Information) or confidential data via electronic communication is prohibited, unless the sharing of the information is necessary due to safety concerns and/or other mandated reporting requirements as indicated by law.

II. **Group messaging**: Staff may never include multiple persons in care in a group text message or email via secure or unsecured platform, even if those individuals attend the same group.

III. **Inactive persons in care:** Staff may not use electronic communication methods to reach out to inactive persons in care.

IV. **Personal number/email**: Staff may not use their personal cell phone number or email to text or email persons in care. Staff should never share their personal phone number or email with persons in care. If a staff member needs to use their personal device to call a person in care, call blocking must be used.

V. **Personal information:** Electronic communication should be treated with the same clinical consideration as verbal communication and should be used as a business tool only for the purposes outlined above. Staff personal information should not be shared with persons in care via electronic communication methods.

VI. **Video chat**: Video chart should not be used with persons in care, except for secure telehealth services provided via separate telehealth platform with appropriate telehealth consent signed by the person in care (see Policy 149).

Note: This is not an exhaustive list, and staff should continue to exercise their professional and clinical judgment when communicating with persons in care via secure text message. If staff have concerns around the use of electronic communication and/or to file a complaint about observed misuse of electronic communication that may require investigation, staff may contact the Compliance Hotline at (831) 755-4018 or anonymously at (866) 262-8616.

Documentation of Electronic Communication

I.   Electronic communication is considered asynchronistic communication and is therefore **not** considered a "direct service."

II.   Interactions with the person in care via electronic communication (i.e. text, email, fax) shall be documented in the electronic health record using the appropriate service code.

III.   Documentation of these exchanges shall still follow the progress note documentation requirements outlined in Policy 23-068 CalAIM - Documentation Requirements for all Specialty Mental Health Services (SMHS), Drug Medi-Cal (DMC), and Drug Medi-Cal Organized Delivery System (DMC-ODS) Services.

<u>Definitions</u>

I. **Confidential Data**: Information that allows public identification (either via direct or indirect identifiers) and may result in harm to an individual or organization if shared unsecured or without authorization.

II. **Electronic Communication**: Communication requiring the use of technology for the purpose of information exchange, including but not limited to text messaging, email, or facsimile.

III. **Encryption/Encrypted Communication**: A process of rendering information indecipherable to protect it from unauthorized view or use by a third party.

IV. **Inactive Client**: A person in care in the MCBH System of Care or contracted provider network for whom services have been terminated, resulting in the closing of clinical record.

V. **County/provider-Approved Secure Text Messaging Platform:** A county/provider-approved application that allows staff members to safely send and receive encrypted text messages. This method is secure, encrypted, and HIPAA compliant.

VI. **Protected Health Information (PHI):** Individually identifiable health information in any form or medium, whether electronic, paper, or oral. This information relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is reasonable basis to believe the information can be used to identify the individual.

VII. **Telehealth**: Refers to services (counseling, rehabilitation, therapy, medication support services, collateral, etc.) provided via telephone and/or secure video/audio call (i.e., Zoom).

VIII. **Texting/Text Messaging:** The act of sending short text messages between cell phones or other mobile devices. Synonymous with Short Message Service (SMS).

IX. **Video Chat:** A face-to-face conversation held over the internet via smartphone, workstation, or webcam.