ADMINISTRATIVE PRACTICES MANUAL

Communication Policy

PURPOSE

To provide procedures for safeguarding Protected Health Information (PHI) transmitted in any form, format or medium, including verbal, written and electronic methods of communication.

PROCEDURE

Verbal

When communicating PHI verbally, workforce members will do so in private settings with lowered voices. If a client/patient name is needed, only the first name will be used. Workforce members should not use a speakerphone when discussing PHI, and when leaving a message, they should leave a simple message without PHI. Workforce members should only note that their department is calling and leave a call-back number. Workforce members can also leave information necessary to confirm an appointment, but should not disclose what the appointment is for. Further, workforce members should not leave any callback numbers or information in a voicemail that would disclose what the service is for or what services are provided. In these instances, Dane County will need to set up a ghost line to mask the actual number so other people cannot search for the number and determine what a service is for.

Mail

When sending mail to clients/patients, workforce members will ensure the recipient's name and address are correct and put in the correct envelopes. If using envelopes with windows, workforce members will ensure no information other than name and address can be viewed. If other information can be viewed, they should use an envelope without a window.

When sending inter-departmental mail containing PHI, put the document in a regular sealed envelope first addressed to the workforce member. The envelope should be marked "confidential" before putting it into inter-department envelope.

Electronic mail (E-mail)

When sending external emails that include PHI, workforce members will send encrypted emails using the following guidelines:

1. Prior to sending an e-mail to a client/patient, containing PHI, the client/patient must give Dane County consent.
    a. Staff should check the client/patient file to verify that there is a completed **Client's/Patient's Right to Request Alternative Communications Form**.
    b. If no form has been completed, a workforce member should obtain verbal consent from the client/patient and then complete the **Client's/Patient's Right to Request Alternative Communications Form.**
2. Emails containing PHI must be encrypted. For encryption to occur:

a. PHMDC workforce members must enter "#secure" in the subject line of an email that contains PHI. The subject line can contain other words, but "#secure" must be somewhere in the subject line. Emails should include discrete, generic subject lines and should not include the client's/patient's name or information about their health or treatment in the subject line. The recipient will receive the email message along with a notice to register a user ID and password, which must be set up in order to access encrypted messages.

    i. Recipients have three days to access the encrypted message. If they have not accessed the email within three days, the workforce member will need to re-send the message using the encryption process.

b. Dane County workforce members must follow DCIM or City of Madison IT protocol and procedures for sending emails securely (see **Proper Use of Computer Equipment, Software, and Connectivity** policy).

3. All emails must contain a confidentiality statement, such as: *"This email, including any attachments, may contain confidential or protected health information, which is only for the intended recipient. If you received this email in error, please delete and notify the sender immediately."*

4. If an external recipient has difficulty opening an encrypted message, that individual should contact the workforce member who sent the message, who will troubleshoot access and contact the Dane County or City IT Helpdesk for assistance if necessary.

Fax

Fax machines should be located in a secure area of Dane County, with no public access. A cover sheet will always be used when faxing client/patient information. Cover sheets should not include any client/patient information. The cover sheet will include the following information:

1. Date of the fax;
2. Recipient's fax number;
3. Name of recipient and their organization
4. Name of sender and their contact information (including phone number);
5. Number of pages being faxed;
6. A confidentiality statement such as: "*CONFIDENTIALITY NOTICE: The information contained in this message is intended only for the private and confidential use of the designated recipient(s) names above, and includes information which should be considered private and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error, and that any review, dissemination, distribution, or copying of this message is strictly prohibited.*

   If you have received this fax message in error, please notify the sender immediately, and dispose of the confidential information properly, e.g., by shredding or by returning it to the sender. Thank you."

7. Whenever possible, auto-faxing should be utilized for reduction of human errors in dialing the fax numbers. Assigned workforce members should routinely check for faxes and distribute them to appropriate personnel.

Texting

Workforce members in covered components are allowed to communicate with clients/patients through text messaging as long as the messages from workforce members do not contain PHI. If a client/patient name is needed, only the first name will be used.

If a workforce member receives any PHI via a text message, they should transfer a copy of the message or photos into the client/patient file, and delete the message from their device. Workforce members should also notify the client/patient that further transmission of any PHI should be done utilizing one of the other methods of communication.

Social Media

Workforce members in covered components are discouraged from communicating with clients/patients through any social media platform or instant messaging forum (Facebook, Instagram, Snapchat, TikTok, WhatsApp, Twitter, Wink, etc.).

If a workforce member receives any PHI via any social media platform, they should transfer a copy of the message or photos into the client/patient file, and delete the message from their device. Workforce members should also notify the client/patient that further transmission of any PHI should be done utilizing one of the other methods of communication.

Mitigation and Breach Reporting

When a workforce member becomes aware of misdirected information, they should follow the Privacy and Security Incident and Breach Policy. If a workforce member receives information in error, that person should contact the sender and immediately dispose of the misdirected information.

DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven (7) years.

ROLES & RESPONSIBILITIES

The HIPAA Privacy & Security Officer is responsible for the implementation, maintenance, and adherence to this policy.

RELATED DOCUMENTS

Definitions
Computer and Portable Media Device Policy
Privacy and Security Incident and Breach Policy
Dane County Social Media Policy
Proper Use of Computer Equipment, Software, and Connectivity
Client's/Patient's Right to Request Alternative Communications Form

DOCUMENT VERSION HISTORY
Original: 08/2023
Reviewed: 07/2024