



EMAILING PROTECTED HEALTH INFORMATION PROTOCOL

OVERVIEW

- It is the policy of the Department of Mental Health and Substance Abuse (DMHSA) to protect the electronic transmission of protected health information (PHI) as well as to fulfill its' duty to protect the confidentiality and integrity of consumer PHI as required by law and professional ethics.
- The Security Rule does not prohibit communication via email or other electronic means (open network), and encryption is not required although it is a good practice to prevent risks associated with emailing PHI.
- Sending PHI by email exposes the PHI to two risks: (1) The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong email address, (2) The email could be captured electronically en route.
 - HIPAA request organizations take reasonable steps to protect against these risks but acknowledges that there must be a balance between the need to secure PHI and the need to ensure that providers can efficiently exchange a consumer's PHI.
- The standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c) (1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to PHI.

DEFINITION

- **PHI:** Protected Health /information, also includes ePHI, Electronic Protected Health Information.
- **Protected Health Information:** Any information, whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse and relates to the past, present, or future physical or mental health or 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.
 - PHI includes any individually identifiable health information. Identifiable refers to a subset of health information, including demographic information. It also includes health information with data items which reasonably could be expected to allow individual identification.

STANDARDS OF CARE

- Email messages, regardless of content, should not be considered secure and private.

EMAILING PROTECTED HEALTH INFORMATION PROTOCOL

- Personal email accounts (AOL, Yahoo, Hotmail, Gmail, etc.) are not permitted for the use of communicating PHI. All DMHSA employees that require the use of email to communicate PHI must do so through a DMHSA managed email account.
- The amount of information in any email will be limited to the minimum necessary to meet the needs of the recipient. Whenever possible, de-identified information will be used.
 - Extraneous comments, opinions, assumptions, and speculations should be excluded from all email correspondences.
- Requests to discuss PHI, not appropriate for email, should be resolved via telephone or in-person.
- Whenever applicable, staff shall make an effort to use a more secure form of communication (i.e., telephone, in-person meeting, repository) to transmit highly sensitive PHI (i.e., Information relating to AIDS/HIV, drug and alcohol abuse, etc.).
- It is good practice to put the PHI in to a Word document, password protect the Word document and attach the Word document to the email, instead of putting the PHI directly in the body of the email.

PROTOCOL

- Email users will be set up with a unique identity complete with unique password and file access controls.
- Email users may not intercept, disclose or assist in intercepting and disclosing email communications.
- Users should verify the accuracy of the email address before sending any PHI and, if possible, use email addresses loaded in the system address book.
- All emails containing PHI must contain a confidentiality statement (example at the end of this protocol).
- Outlook calendar appointments should not use a consumer's full name to identify the meeting.
- Users should exercise extreme caution when forwarding messages.
- Users should never automatically forward his/her DMHSA email account to any non-DMHSA account, including but not limited to, personal and commercial email accounts such as AOL, Hotmail, Yahoo, MSN, Gmail, etc.
 - Staff can access their DMHSA email from any computer by going to mail.dmhsa.guam.gov/exchange

EMAILING PROTECTED HEALTH INFORMATION PROTOCOL

- PHI should not be sent to a distribution list (i.e., DMHSA Administrators, DMHSA Supervisors, DMHSA Social Workers, etc.).
 - Instead, each recipient should be listed individually.
- Users should periodically delete email messages that are no longer needed.
 - Instead of saving the PHI in the email system, staff shall print and appropriately store hard copies of the information.
- The Subject/'RE' part of an email should never identify the consumer (i.e., initials, medical record number, name, etc.) or included PHI.

Emailing PHI on the Internal Network:

- PHI may be sent within the internal network of DMHSA.
- Whenever possible, staff shall avoid transmitting highly sensitive PHI (i.e., Information relating to AIDS/HIV, drug and alcohol abuse, etc.) by email on the internal network.
 - When applicable, staff shall make an effort to use a more secure form of communication (i.e., telephone, in-person meeting, repository) to transmit highly sensitive PHI.

Emailing PHI outside of the Internal Network:

- Staff may exchange PHI outside of the internal network by email, as long as they follow the rules.
- Generally, the only reason PHI should be sent by email outside of the internal network is because the PHI is urgently needed for consumer care or the PHI must be transmitted in a timely manner.
- The safest way to send an email outside of the internal network is to encrypt the email. (Outlook is not encrypted).
- When sending PHI outside of DMHSA internal network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information.
 - To secure the confidentiality emails should limit the amount of direct identifiers (name, address, social security number, date of birth, phone numbers).
 - Less direct identifiers such as the medical record number and initials may be included.
- A consumer's highly sensitive information (i.e., drug and alcohol, HIV/STD related information, etc.) must not be emailed to any party outside the internal network without using security safeguards.

EMAILING PROTECTED HEALTH INFORMATION PROTOCOL

- Sample security measures include password protecting the document(s) in a Word document and attaching it to the email and/or encrypting the message.
- When replying to emails containing PHI from senders outside of the DMHSA network, the response may not contain the original message.

Receiving an Email Containing PHI in Error:

- Staff shall send a new email (do not hit reply or reply all) noting that he/she received the email in error and that the sender should check that he/she has the correct email address.

Termination and Reporting Violations:

- Employee email access privileges will be removed promptly following his/her departure from DMHSA.
- Employees should immediately report any violations of this protocol to his/her Supervisor or the Director.

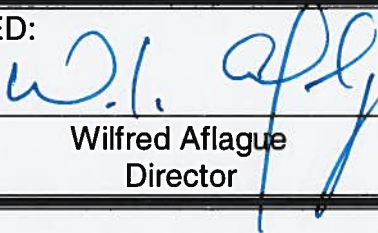
Sample Confidentiality Statement:

The information contained in this e-mail, including any attachments, is legally privileged and confidential information intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any viewing, dissemination, distribution, or copy of this e-mail message is strictly prohibited. If you have received and/or are viewing this e-mail in error, please immediately notify the sender by reply e-mail, and delete this e-mail from your system. Thank you.

REFERENCES

- 45 CFR § 164.312(a)
- 45 CFR § 164.312(c)(1)
- 45 CFR § 164.312(e)(1)
- 45 CFR § 160.103

APPROVED:



Wilfred Aflague
Director

Date: 