POLICIES & PROCEDURES		
Series	PRIVACY & SECURITY	
Title	EMAIL & PHI	
Policy Date	05/2013	**Procedure Date:** 11/2013

TABLE OF CONTENTS

POLICY

Valley Mental Health, Inc. (VMH) will not transmit protected health information (PHI) by email unless the sender is using a secure e-mail system.

REFERENCES

45 CFR § 164.312(e) and 164.530(c)

Electronic Transmission Security of PHI

Accounting of Disclosures of Health Information

PROCEDURES

A. Risk Assessment & Committee Responsibilities

1. The Security Officer will gather all information collected for the risk assessment process relating to email usage. This assures that the processes chosen to carry out the email usage protocol are in accordance with the level of risk, priority, and importance assessed by VMH.

2. The Security Officer will establish a committee comprised of the following (as necessary and applicable), or their designees:

   - Designated Security Officer (chair)
   - Designated Privacy Officer
   - Chief Information Officer
   - Director of Human Resources
   - Representatives from affected business areas

3. The committee is responsible to choose the VMH preferred technical solution and process to develop the procedures which function to reasonably safeguard VMH protected health information, and make up email usage protocol by considering the following factors:

a. Reviewing the risk assessment results and related documentation

b. Investigating technical solutions or products designed to meet the goals of the policy. This investigation process includes reviewing resource requirements and considering associated costs of the solution.

c. Balancing the confidentiality of the protected health information, with the ability of the solution to allow for data integrity and availability.

d. Thoroughly considering all areas defined in the procedure as "Implementation Considerations."

4. The chair of the committee will assure that all decisions related to the solution(s) chosen are well documented and retained in accordance with VMH retention policy.

5. Once a process and/or technical solution is chosen, the Security Officer will work with the committee to ensure the various related implementation subtasks are appropriately assigned allowing for a realistic implementation process.

6. The Security Officer will additionally assure that any and all related policies and procedures will be updated, including training materials.

7. To the extent that workforce functions are affected by the chosen solution, the training department will work with managers to coordinate and assure that the solution is implemented and each affected member is trained.

8. The Security Officer will ensure that routine monitoring of this solution is carried out on an as needed basis but no longer than annually in order to continually assess the effectiveness of VMH's ability to balance the confidentiality of the protected health information with its integrity and availability. Additional modifications will be made to this policy to improve the security of electronic communication involving the transmission of protected health information.

B. How to Send Encrypted E-mail & Practices

1. Protected health information may not be transmitted by e-mail unless the sender is using a secure VMH e-mail system (see 2 below). PHI must not be forwarded externally to personal e-mail accounts.

2. To send an encrypted email, type "secret" as the first word in the subject line. You can include additional unidentifiable text following a single space. The subject line must not contain PHI information.

3. VMH has software that includes security rules to identify social security numbers, date of birth, etc. If the system finds matching data when sending an e-mail externally, it will not send the email. This software is an extra measure to prevent PHI from going out externally without proper use of "secret" in the subject line. Therefore, all staff are to use the process in number two above to send encrypted e-mail.

4. Do not use secure e-mail to send a message to more than one client at one time. This is to avoid the potential for inadvertent disclosure of e-mail addresses, linking e-mail

addresses with clinical information in the message, or violating prohibitions against using client-specific information for certain types of marketing.

5. Any form of messaging is not secure and may not be used to transmit protected health information. This includes, unsecured texting, Instant messaging, any social media, chatting, blogging, twitter, etc.

C. Communications with the Client or Others.

1. There might be times when the provider is asked by the client to communicate by e-mail. When this happens, the provider will use the VMH secure e-mail system.

2. Communications with clients or others involved in the client's care may be subject to inclusion in the client's record. When transmitting to a client or other individual and the content contains PHI, the message must be sent encrypted. Not doing so will result in an inadvertent or incidental disclosure. These types of disclosures require entry in the Accounting of Disclosures of Health Information and are reported to the Privacy Officer.

D. Communications Containing PHI – Not Directed to Client

1. There are times when workforce members, as part of their task functions, must create or have access to documents containing PHI. This could be in the form of a spreadsheet containing multiple client names or other work-flow procedures that must be shared.

2. When the distribution is internal, encryption is not required, however, use caution to send only to those who have authority to receive the information. Broadcast e-mails have the inherent consequence of reaching audiences who should not have access to that information.

3. When reports or forms with PHI are e-mailed to an external destination, these must be sent encrypted. Not doing so will result in an inadvertent or incidental disclosure. These types of discourse require entry in the Accounting of Disclosures of Health Information and are reported to the Privacy Officer.

E. Secure E-Mail System Features

1. Transmission Security: The message cannot be intercepted. The message is sent encrypted over an open network (e.g. the internet). VMH encryption Standards are approved by the Security Officer.

2. Mechanism to Authenticate: The recipient of the message will know that the content has not been altered or destroyed during transmission.

3. Person or Entity authentication: The recipient of the message will know the true identity of the sender.

4. Integrity Controls: There are safeguards to lessen the possibility of sending the message to someone who is not authorized to receive it. There are safeguards to reduce the likelihood that the message will be forwarded to someone who is not an intended recipient.

5. Encryption: Encryption is a mechanism to encrypt or transform confidential plaintext into ciphertext in order to protect it. An encryption algorithm provides the process to

transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Encryption is listed as addressable to be used “whenever appropriate” in the final security regulations.

F. Managing E-Mail System

1. The Security Officer, with the assistance of the Chief Information Officer and others with expertise in secure e-mail systems, as necessary, will develop modifications to the VMH e-mail procedure.

2. The modifications will address internal communications among members of the workforce, communications with clients, communications with insurance companies, and other e-mail uses that involve the use of PHI.

3. De-activating encryption system for an individual

   a. The Security Officer will receive all requests for deactivating encryption software for any VMH staff.

      (1) The Security Officer in conjunction with Information Systems Director will make the following considerations prior to deactivating encryption capabilities:

         (a) Determine if the individual works with PHI on a regular basis. If yes, deactivation is not granted

         (b) Does the individual understand the implications of sending unsecure PHI.

            (i) Individual must read, understand and sign the Deactivation of E-mail Encryption Acknowledgement Form.

            (ii) The form reviewed by participating staff and signed on an annual basis

         (c) Present request and coordinate Executive Leadership Team (ELT) approval prior to deactivating encryption.

         (d) Documentation of the request, acknowledgment, and ELT approval is maintained by the Security Officer or designee.

G. Workforce Accountability: Positive Email Usage Protocol

1. Do use email responsibly and productively to facilitate VMH business and maintain and enhance the organization’s image and reputation

2. Actively monitor and manage email mailbox contents; periodically delete non-record messages no longer needed for reference; set the e-mail preference to automatically delete deleted messages

3. Keep all external distribution and e-mail addresses updated to avoid misdirection of information

4. Compress large files or documents using a tool like Winzip before attaching to an e-mail message; often a message exceeding 2 mega-bites may be returned as undeliverable

5. Keep a copy either in an e-mail mailbox folder, or a paper copy print out of any business record that originate through e-mail as long as the printed email does not contain PHI. If printed email contains PHI it must be stored in a secured location and not transported externally of any VMH facility.

H. Workforce Accountability: Email Use to Avoid / A Message for the Workforce

1. Do not use “Instant Message” programs as they are inherently not secure

2. Do not send any e-mail message that you would be embarrassed to find printed under your name on the front page of your local paper

3. When replying to an e-mail, do not include the prior message(s) in your response if the prior message(s) may contains PHI or other confidential information which either you or your recipient have copied or forwarded the information

4. Only use the reply and reply-all feature when you are aware of the number and identity of the recipients and that the return transmission is secured and encrypted if sending to an external source.

5. Do not use graphics, clip art or other large images or backgrounds in your e-mail messages or e-mail signature; this speeds up delivery and saves space in your e-mail mailbox

6. Personal use of e-mail should be limited and may not interfere with your work duties

7. Never use profanity in mail messages

8. Never distribute information that is obscene, abusive, libelous or defamatory

9. Do not distribute copyrighted material without written permission

10. Do not impersonate another user

11. Never access another’s e-mail account

12. Do not send chain letters; these use vast system resources

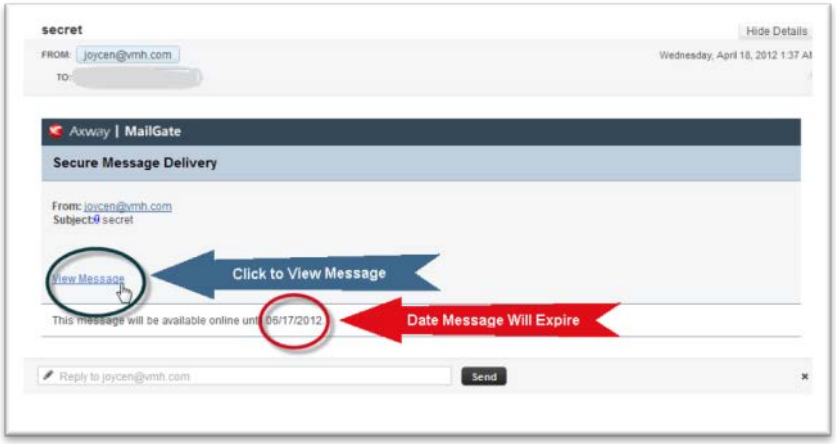
13. Do not use all capital letters; this is like shouting in writing

14. Do not send e-mail messages to distribution lists unless you understand the purpose and the membership of the list

15. Do not send e-mails with legally sensitive, or controversial subject matter. This information should be communicated in person or by telephone.

I. VMH’s Encryption System – Recipient’s view

1. Below is an example of what your recipient will see in their Inbox.



2. Below is an example of the protected message itself, viewed via web browser using a secure web connection. The recipient only has to click the link in the secure message (ie, the example shown above) in order to view your message.