

Compliance Education

HIPAA Tip Sheet: Email

HIPAA regulations require special care of Protected Health Information (PHI) in all written, verbal, and electronic messaging – including email. Email is an important and efficient method of communicating in the workplace, but patient/member privacy and confidentiality must always be protected.

Sending Emails:

- Only use your VNS Health email for VNS Health business
 - Do not use personal email domains such as Gmail and Yahoo
- Encrypt all emails containing PHI when the email recipient is not a part of the 'vnshealth.org' domain
 - To encrypt, type *ENCRYPTME* anywhere in the subject line **or** click *Options>Encrypt>Encrypt-Only* in the email itself
 - If sending emails to any secure email partners on the [TLS](#) Partners List, there is no need to encrypt
- Follow any [Data Loss Prevention \(DLP\)](#) warnings that pop up when sending large amounts of PHI/PII
- Verify email recipients:
 - Double check the accuracy of every email addressee
 - Be careful when selecting from an auto-populated list of email addresses
 - Do not automatically select "Reply all" on emails containing PHI; only include recipients that need to access the PHI – and always remember to encrypt emails to non-VNS Health recipients
- Follow the [Minimum Necessary Rule](#):
 - Only include PHI that is absolutely necessary for the intended purpose
 - Double check that any attachments selected are correct
- Do not include PHI in the subject line of emails
 - Examples: patient/member names, medical record numbers, insurance numbers, etc.

Receiving Emails:

- Don't be a victim of phishing attacks
 - Look for the email warning: "**WARNING: This email arrived from a source external to VNS Health. Please validate the sender and the message content before clicking links or opening attachments.**"
 - Be wary of unfamiliar email senders, emails from VNS Health leaders written with grammatical errors, and email addresses ending in *.biz* or *.com*
 - For more information on how to spot a phishing attack, and on what to do, see the [Phishing Tip Sheet](#)
- Alert patients/members to the risk of sending PHI through email and contact your manager or the HIPAA and Privacy Team with any concerns

What To Do If You Make a Mistake:

- If you send an email with PHI to the wrong VNS Health recipient, recall the email immediately. If the recall is unsuccessful, request that the unintended recipient delete it permanently, and report the incident to your supervisor and the HIPAA and Privacy Team.
- If you send an encrypted or unencrypted email with PHI to the wrong non-VNS Health recipient, immediately request that the recipient delete the email permanently, and report the incident to your supervisor and the HIPAA and Privacy Team.

Rev: 1/2024

For routine HIPAA questions, please contact the HIPAA and Privacy Team at: HIPAA@vnshealth.org
Report potential violations via web at www.vnshealth.ethicspoint.com or
via the **VNS Health Compliance Hotline at 1-888-634-1558**