

## Issues or Concerns?

We want to hear from you. Ask questions and report suspicious activity.

You can always report an issue anonymously.

VNS Health Compliance Hotline:

Phone Number: **888-634-1558**

Online Form: [www.vnshealth.ethicspoint.com](http://www.vnshealth.ethicspoint.com)

To contact the HIPAA Compliance Team,  
by email: [HIPAA@vnshealth.org](mailto:HIPAA@vnshealth.org)

**Annie Miyazaki-Grant,**  
Chief Compliance and Privacy Officer



## HIPAA Pocket Guide


Keep your patients' and members'  
information protected

## What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that sets standards for the verbal, written or electronic exchange, privacy and security of health information.

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) revised certain parts of HIPAA, including the addition of breach reporting requirements, and significantly increased penalties.

## Key Terms to Remember

- **PHI:** Protected Health Information, which includes any information that can identify a patient/member
- **PII:** Personally Identifiable Information which is any information that can be used to distinguish or trace an individual's identity
- **HITECH Act:** along with HIPAA, regulates the privacy and security of electronic PHI
- **Confidentiality:** not revealing PHI to an unauthorized person
- **CTRL/ALT/DELETE or  +L** use to lock your computer or laptop when you step away to secure PHI on your computer
- **ENCRYPTME:** type this in the subject line of any email you want to make secure



## Minimum Necessary Rule

When using, disclosing or requesting PHI, you must make reasonable efforts to limit the use, disclosure or request to **the minimum** amount of PHI **necessary** to accomplish your intended purpose.

### **With co-workers, keep sharing to a minimum.**

Share PHI only if necessary for them to do their job and do not provide more than what is requested and required.

### **With others, do not share without authorization.**

Refrain from discussing patient/member information with family members unless you have specific authorization.

**Never access medical records of family, friends or others** (including celebrities) unless you have proper authorization.

## Some PHI is Subject to a Higher Standard

### **Individuals protected include those who are:**

- Living with HIV, AIDS or related diseases, taking HIV medications, exposed to HIV or testing for HIV
- Needle-sharing partners or children of a protected individual
- Living with mental health, alcohol and/or substance abuse issues


### **You must limit sharing of HIV, mental health, and addiction-related information to:**

- Staff with a reasonable need to know
- Providers when necessary to provide care or services
- Person(s) with expressed written authorization from patient/member

### **If you are uncertain about releasing sensitive information (including HIV-related),**

contact your supervisor or VNS Health's HIPAA Compliance Team.

## Follow Security Rules

- Keep passwords and logins/usernames unique and never share. Never post on devices
- Close programs when not in use
- Lock unattended computers: (1) Ctrl-Alt-Del > Select Lock or (2)  + L.
- Secure electronics out of sight or in a locked car trunk while in the field or traveling. Avoid putting electronics in your pocket or carrying when in transit
- Ensure that PHI stored on removable storage is encrypted—contact the IT Help Desk for assistance
- Avoid suspicious emails and report any that you receive to IT

If your VNS Health-issued device is stolen or lost, report it immediately to IT by calling **212-290-3555** or Report an Issue via the IT Self Service Portal and select Security Incident within the “Service Impacted” field, select Lost/Stolen within the “Service Category” field as part of completing the rest of the form. Report lost/stolen device to your manager and email the HIPAA Compliance Team at [HIPAA@vnshealth.org](mailto:HIPAA@vnshealth.org).

## Protect Paper PHI

- All paper PHI should be shredded or disposed of in office shredding bins and not in the regular trash
- Avoid keeping or carrying paper PHI. Only take the documents that are needed to do your job. Eliminate identifiers whenever possible
- Use confidential cover sheets containing the HIPAA confidentiality clause when faxing
- Avoid posting PHI in public or common areas and keep PHI out of view when working remotely
- Collect all paper before leaving patient/member home. Do not leave PHI unattended at the office or remote work space
- If in the field, store PHI in your zippered bag or locked trunk
- If working remotely, store PHI in a locked drawer or cabinet
- Double check patient/member name and address when mailing PHI or leaving documents in the home
- Avoid printing PHI whenever possible

## Protect Emailed PHI

- Double-check email addresses before sending to avoid sending to unintended recipients
- Be careful when using “Reply All” and avoid sending emails to unnecessary recipients—take anyone off who doesn’t need the PHI or consider deleting the PHI if it is not needed
- Encrypt emails sent outside of VNS Health by (1) typing ENCRYPTME in “Subject” line or (2) clicking Options>Encrypt>Encrypt Only
- Do not open attachments that you did not expect or from senders you do not know—pay special attention to attachments with the incoming email warning “This email arrived from a source external to VNS Health”
- Do not include patient’s name or other PHI in the subject line of emails
- Be mindful of DLP (Data Loss Prevention) program tips and warnings when PII or PHI identifiers have been detected in email sent outside of VNS Health. For example, if 100 or more unique PII or PHI identifiers have been detected in an email going outside of VNS Health, you will be allowed to send only using Outlook Message Encryption
- Do not send, receive or forward confidential work emails to your personal device or email account
- Alert patients/members to the risks of sending PHI through email and contact your manager or the HIPAA team if you have any concerns

## Limit Verbal PHI

### Speak softly and avoid public places

- When possible, obtain permission before disclosing information to family or others in person or on the phone
- Limit to the minimum necessary information, including on voicemail and answering machines
- Ensure PHI cannot be overheard by others, including family/friends. For example, utilize head phones, close doors, avoid working in public areas (e.g., trains or buses).
- Take measures to avoid disclosing PHI to others when video conferencing using Microsoft Teams or Zoom.

### Texting tips

- Texting must be secure—only use VNS Health approved devices and platforms such as **Tiger Connect**
- Never use your personal device to send text messages to share PHI unless authorized