

Compliance Education

HIPAA Tip Sheet: Remote Working

While working remotely, all members of the VNS Health workforce must ensure the continued security of Protected Health Information (PHI) and electronic PHI (ePHI) while working remotely. All VNS Health HIPAA and Information Security policies/procedures remain in effect. See [VNS Remote Work Policy](#)

Verbal PHI

- Identify a location in your home that ensures PHI cannot be overheard by others; close doors, use a low voice; use headphones especially during Fortifone/Zoom/Teams calls and meetings
- Use non-verbal communication including Chat tools in Microsoft teams whenever possible
- Avoid discussion of PHI in public areas including trains and buses

Chat and Collaboration

- Use only company approved software for online meetings/chat discussions of PHI
- Online meetings or chat discussions containing PHI should not be recorded or stored
- Do not use texting to share PHI unless using an approved secure platform e.g., Tiger Connect

Email Security

- Never share your VNS Health user ID or passwords with anyone
- Always decline the option to stay logged into your VNS Health email on shared computers
- Email should not be used as storage for ePHI; transfer and store email in a secure file

Remote Access

- Use approved methods for remote connection to the VNS Health network including VPN access
- Devices including laptops, tablets, cell phones, and any other smart devices should comply with the *VNS Health HIPAA Security Policies & Procedures*
- Any device used for remote access must not be shared with anyone outside of VNS Health
- Store VNS Health electronic devices in a secure location not accessible to others
- PHI should not be stored on personally owned devices; the use of personal devices is subject to the [VNS Health Bring Your Own Device Policy](#)
- **Paper PHI**
- Limit use of paper-based PHI; consider scanning important documents
- When paper-based PHI must be created or transported, retain in a locked cabinet or room
- Refrain from printing, faxing, or copying paper-based PHI whenever possible or do so minimally
- Dispose of paper-based PHI in VNS Health shredding bins or in a portable home shredder

Notify the Compliance Department and IT of all Lost/Stolen devices and /or other security incidents.

(Rev. 5/2023)

For routine HIPAA questions, please contact the HIPAA and Privacy Team at their email:

HIPAAandPrivacy.Team@vnshealth.org

Report potential violations via web at www.vnshealth.ethicspoint.com or

VNS Health Compliance Hotline at 1-888-634-1558