VNS HEALTH CORPORATE
POLICY & PROCEDURE

TITLE: Remote Work Policy

APPLIES TO: VNS Health Home Care, including the Home Care, and Care Management Organization (CMO) divisions;
VNS Health Personal Care;
VNS Health Behavioral Health, Inc.;
VNS Health Health Plans;
VNS Health Hospice Care; and
Medical Care at Home, P.C. (collectively, "VNS Health")

POLICY OWNER: Corporate Compliance Department

FIRST ISSUED: March 2022

NUMBER: HIPAA. 23

PURPOSE

VNS Health will provide eligible employees with the option of working remotely at different frequencies.[1] While working remotely, all members of the VNS Health Workforce must ensure the continued security of Protected Health Information ("PHI") and electronic PHI ("ePHI"). All VNS Health HIPAA and Information Security policies and procedures, including those for handling physical and electronic PHI, remain in effect as if the Workforce Member was working onsite.

POLICY AND PROCEDURE

I. Protecting Discussions Involving PHI

A. Workforce Members shall identify a location within their home from which they can discuss PHI with co-workers, health care entities, vendors, patients, members, and others. Consider modes of non-verbal communication such as the chat tools in Microsoft Teams.

II. Protecting Paper-Based PHI

A. Workforce Members shall limit the removal of paper-based PHI from VNS Health workspaces whenever possible. Instead, Workforce members shall consider secure alternatives to transporting paper, such as scanning the documents before working from home and storing them in a secured

[1] See *VNS Health Virtual Work Policy* that describes the different work models, e.g., on-site, hybrid, and mostly virtual.

network drive.

B. If paper-based PHI must be transported to the home environment or created at home, the Workforce Member is obligated to ensure the physical security of PHI by following the "2-key concept." The "2-key concept" means PHI at rest is stored in a locked "container" within a locked environment. For example, PHI can be stored in a locked drawer cabinet or room, which is then stored within a locked home.

C. Workforce Members shall refrain from printing, faxing or copying any documentation that contains PHI; if it is necessary to print, fax or copy a document that contains PHI, Workforce Members shall print, fax or copy minimally.

D. Paper-based PHI no longer needed for the intended purpose should be returned to VNS Health for proper disposal and shredding. In general, Workforce Members who work partially remotely are prohibited from disposing of documents containing PHI utilizing home disposal methods, even if the documents are shredded first. However, for those Workforce Members who have been granted the option to work fully remotely, documents containing PHI must be securely shredded prior to disposal.

III. Chat and Collaboration

A. Workforce Members shall use VNS Health -approved collaboration software solutions, as set forth in Appendix A, to have online meetings or chat discussions concerning patient or member information.

B. Online meetings or chat discussions concerning patient or member information may not be recorded and stored.

C. Workforce Members shall not use mobile Simple Messaging Service (SMS) text messaging to communicate any PHI, unless it is through a VNS Health -approved secure text messaging platform.

IV. File Sharing

A. Departmental file shares through VNS Health -approved collaboration software solutions, as set forth in Appendix A, are approved for sharing files that contain PHI. When using these services, please be aware that Workforce Members should generally save documents containing PHI in these environments and should generally refrain from saving documents containing PHI locally on their computers.

V. Remote Access

A. VNS Health has established approved methods for remotely connecting to the VNS Health network, including through VPN access.

B. It is the responsibility of anyone with remote access to ensure that the device complies with the Workstation Use procedures set forth in the *VNS Health HIPAA Security Policies & Procedures – Workstation Use*.

C. Any device (e.g., laptop, tablet, cell phone or other smart device) used for remote access must not be shared with anyone outside of VNS Health, not

even family members.

D. VNS Health -issued equipment and materials must be stored in in a secure location and not available for use by others, or used for purposes other than MSO business.

E. If Workforce Members have a work-issued laptop or tablet, it should be used to conduct VNS Health business while working remotely, in accordance with the *VNS Health Enterprise Owned Device Policy*.

F. If Workforce Members use personal devices, the device must be compliant with the *VNS Health Bring Your Own Device Policy*.

G. As required by state, federal and industry regulation, if not using a VNS Health -issued device, Workforce Members must connect to the VNS Health network with personal devices that are encrypted and able to receive vendor updates and patches. These protections aim to reduce the risk of VNS Health information being stored or accessed from devices that may not be able to secure the information.

H. Workforce Members will not store PHI on personally owned devices. If there is a business need to store PHI on a personally owned device, it must be encrypted pursuant to VNS Health's *HIPAA Security Rule Policies & Procedures*; and as soon as practical must be transferred to a secure file sharing location and all copies deleted from the personal device. Failure to comply with VNS Health's HIPAA policies will result in sanctions.

I. VNS Health reserves the right to update and require any additional controls for personal devices based upon the risk to the VNS Health network or environment.

VI. Email Security

A. Workforce Members should never provide their VNS Health user ID and password to anyone through email or over the phone.

B. Workforce Members should refrain from selecting any options to stay logged in to their email accounts on computers that are shared or being used for remote work.

C. Workforce Members should not use email as a storage location for ePHI and should transfer ePHI received to a secure file sharing location.

VII. Notification of Security or Privacy Incidents

A. Workforce Members have an ongoing requirement to report information security and privacy related incidents immediately to the Privacy Officer.

VIII. Compliance

A. Failure to comply with this policy will result in disciplinary actions as per the *VNS Health HIPAA Complaints and Sanctions Policy*.

IX. Documentation

A. VNS Health will maintain any documentation evidencing compliance with this policy for six (6) years.

References: 45 C.F.R. §§ 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.310(a)(1), 164.310(c), 164.312(a)(1), 164.312(e)

Reviewed:	3/2022	6/2023						
Revised & Approved:	6/2022	9/2023						

Appendix A: VNS Health Collaboration Tools

Tool	Used for	What is required?	How to get set up?	How to get support?	Notes
Verizon Conferencing	Telephone audio conferencing (only).	• Must be assigned a bridge number. • Telephone to call in.	• IT Service Ticket • Verizon Conferencing Portal to change options	• Verizon Conferencing Portal • Dial *0 in conference	• 500+ current accounts assigned • Up to 50 meeting participant limit • Cost is based on minutes
Microsoft Teams	• Computer audio, video conferencing • Screensharing. • Direct text chat • Teams' channels chat and sharing • File Sharing • Collaboration with non- VNS Health users • Integration with other Office 365 apps • Session Recording • Telephone audio conferencing (Office 365 E5 License required)	• *Audio*: Computer Microphone + Speakers • *Video*: Webcam • *Screensharing/Create Outlook Meetings*: Teams app installed • *Viewing/Joining*: Any web browser • *Telephone Audio Meeting Hosting*: Office 365 E5 License (Directors and above, or as approved)	IT Service Ticket to • Get Teams app installed* • Get E5 License assigned** • Allow collaboration with external users *IT is pushing the Teams app to all VNS Health computers. **Office 365 E5 License is required for	IT Service Ticket	• Replacing Skype. • Available on mobile devices. • 250 meeting participant limit • 5000 members limit in a Team (chat and sharing) • Cost included in Office 365 • Telephony requires E5 license

			telephone conferencing.		
Microsoft Skype	• Computer audio, video conferencing. • Screensharing. • Direct text chat • Telephone audio conferencing (Office 365 E5 License required)	• *Audio*: Computer Microphone + Speakers • *Video*: Webcam • *Screensharing/Create Outlook Meetings*: Skype app installed • *Viewing/Joining*: any web browser • *Telephone Audio Meeting Hosting*: Office365 E5 License (Directors and above, or as approved)	Skype is installed on all VNS Health Computers. Office 365 E5 License required for telephone conferencing.	IT Service Ticket	• Skype is being replaced by Teams. • Available on mobile devices. • 250 meeting participant limit • Cost included in Office 365 • Telephony requires E5 license
WebEx Meeting Center	• Telephone/computer audio, video conferencing. • Screensharing. • Text chat within a meeting • Session Recording • Meet with non- VNS Health users.	• WebEx Meeting Center license and user account • *Audio*: Microphone + Speakers or Telephone • *Video*: Webcam • *Screensharing/Viewing/Joining:* compatible web browser	• Email: Paul Vandeyar	• Email: Paul Vandeyar	• 80+ Licenses currently • Available on mobile devices. • 1000 meeting participant limit • Cost is per license and per minute • Accounts disabled after 30-days of non-use