VNS HEALTH CORPORATE POLICY & PROCEDURE

TITLE: Safeguards 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: May 27, 2009

NUMBER: HIPAA.13

PURPOSE

VNS Health has put into place appropriate administrative, physical and technical safeguards to prevent the intentional or unintentional use of disclosure of protected health information (PHI) in violation of Covered Entity policy or applicable law. VNS Health's workforce and business associates (collectively, "Personnel") will be expected take comply with these steps to reasonably safeguard PHI.

POLICY

A. Administrative Safeguards

1. Policies. VNS Health has implemented administrative policies to address the privacy and security requirements under HIPAA. Such policies are located at VNS Health Intranet Policies & Procedures site. VNS Health Chief Compliance and Privacy Officer (Privacy Officer), or designee, will review this policy periodically and update as needed.

2. Oral Communications. Personnel must exercise due care to avoid unnecessary disclosures of PHI through oral communications and pay attention to unauthorized listeners. In addition, Personnel must not:

(a) discuss PHI in public areas, including elevators or lunchrooms.

(b) discuss or disclose PHI outside of VNS Health.

(c) discuss patients or members with other Personnel unless they have a job-related reason to do so.

3. Facsimiles. Facsimile transmissions of PHI are permissible. To protect the confidentiality of PHI and reduce the risk of unauthorized receipt of a fax, Personnel will be instructed to take the following steps:

(a) Verify the correct fax number.

(b) When reasonable, contact the recipient of the PHI to ensure that the recipient knows that the fax is coming and arrange for its timely pick up from the fax machine.

(c) When reasonable, check the fax transmittal summary, log and/or fax confirmation sheet to ensure that the fax was sent to the correct recipient(s). If the sender determines that the fax was erroneously received by an unauthorized recipient, the sender must take steps to immediately contact the unintended recipient and ask that the fax be destroyed. The sender also must document the erroneous transmission, record the date and events, and inform their supervisor of the error, who must inform the Privacy Officer.

(d) Locate fax machines in areas that are secured, and not accessible to the public.

(e) Check fax machines to assure that faxes containing PHI are not left unattended in the machine.

(f) Send facsimile transmissions with a fax cover sheet that includes a confidentiality statement.

4. Telephone Protocols.

(a) Personnel will not discuss PHI over the phone until the following can be confirmed:

(i) The identity of the caller.

(ii) Verification that the caller has the need to know the requested information and that the disclosure of PHI is permissible.

(b) Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient or member has requested and received approval for an alternative means of

communication. However, the amount of PHI that is left must be limited. Telephone messages regarding test results or that contain information that links a patient's or member's name to a medical condition should be avoided.

5. Texting. PHI may only be communicated via text message if text messages are sent using a VNS Health issued or approved mobile device which encrypts data while at rest; and using a secure, VNS Health approved texting service which encrypts data while in transit.

(a) Clinician-to-clinician text message communications may include PHI; however, physician orders may not be communicated by text.

(b) VNS Health clinicians and other staff members are not permitted to communicate PHI via text messaging to patients, members, clients or their respective family members. Text messages must be sent solely to communicate scheduling and confirm appointments or other non-clinical information. These text messages should contain the minimum amount of information necessary to communicate with the patient, client, and member, or their respective family members, or other VNS Health staff members. Medical and health-related PHI is prohibited from being sent via text message.

(c) Text message communications must comply with the relevant text message policies.

6. Disposal. PHI will be disposed in a manner to make it unreadable and unusable. For example, paper records will be shredded; electronic media must be erased before disposal, per the Procedures for Media Disposal. Electronic PHI must be deleted from information systems when there is no longer a business or clinical need to access such information by following the Decommissioning Procedure.

7. Media Re-Use. Any electronic PHI residing on electronic media (e.g., tapes) must be removed following the Decommissioning Procedure before re-use.

8. Remote Work Areas. The following safeguards will be put into place when Personnel are working remotely:

(a) PHI will not be removed from VNS Health unless authorized and required for Personnel to perform their job functions.

(b) Personnel will ensure the privacy and security of remote work areas, including locked remote (home) offices, locked file cabinets and locked desks.

(c) If permitted to remove PHI, Personnel will secure PHI when in transit, (e.g., Do not leave PHI unattended in a car or, if information must be kept in the car, store it in the trunk, lockable attaches, lock boxes, or other

secure opaque containers).

Personnel will not download electronic PHI onto computers in remote locations (e.g., on hotel computers).

9. Additional Considerations. In addition to the administrative safeguards discussed above, VNS Health Personnel will comply with the following safeguards:

(a) Sign-in sheets that are viewed by multiple patients or persons will not contain health information (e.g., reason for visit) and unnecessary identification information (e.g., address, Social Security Number).

(b) Patient/member records used by Personnel for their job functions in shared workspaces will be reasonably protected to prevent inadvertent disclosures. This may include placing a cover sheet over records sitting on a desk or positioning a patient/member record so that the patient/member name is not visible.

B. Technical Safeguards

1. Email. All e-mail transmissions containing PHI must be encrypted. VNS Health encrypts all outgoing email when traversing the Internet, with minimal exceptions. VNS Health also enforces additional protections when PHI is detected by our email systems. In addition, Personnel must comply with the following safeguards:

(a) E-mails will be reviewed to ensure that they are addressed to the correct recipient.

(b) Senders contact information will be included on the e-mail.

(c) Where practical, the e-mail will be labeled according to the Data Classification Policy.

(d) Senders will read and follow "Tips" displayed when PHI is accurately detected.

(e) Senders will use the Outlook Message Encryption (OME) method when sending PHI, unless a "Secure Email Partnership" has been established with all receiving parties. OME is enforced when "ENCRYPTME" is in the Subject line of the email or when the "Encrypt-Only" permission is used.

2. Access Controls.

(a) VNS Health's computer systems are to be used only by those individuals authorized to do so through the policies of VNS Health. The Access Control Policy governs access to information systems.

(b) Personnel will be assigned user IDs/passwords for access authorizations to electronic PHI. Authorization to access electronic PHI will be based on the person's job responsibilities. Authorization to access a workstation, transaction, program or process will be modified upon a change in the person's job function.

(c) All passwords must be constructed in compliance with the Basic Password Policy.

(d) Personnel are not permitted to share passwords.

(e) Upon termination of a Personnel member, their user ID/password will be promptly disabled.

(f) Only authorized Personnel, including authorized third-party maintenance personnel, may access software programs for testing and revision.

See also, additional IT Policies available at the VNS Health Intranet Policies & Procedures site.

3. Workstation Use: VNS Health must maintain secure workstations to eliminate or minimize the possibility of unauthorized access to both PHI and electronic PHI. Personnel must exercise prudence and common sense to maintain the security of information accessible from their workstations. Workstations include computer terminals, laptop computers, mobile tablets and smartphones. At a minimum the following procedures should be followed:

(a) Workstations must be protected using the "Physical Access" controls required by the Access Control Policy.

(b) Printing and copying of documents with electronic PHI should only occur to the extent necessary.

(c) Electronic PHI may only be downloaded to approved, encrypted workstations with proper authorization.

(d) If electronic PHI is properly downloaded to a portable workstation, to the extent possible, only the minimum amount of information necessary for the Personnel's job function may be downloaded.

4. Use of Social Media Sites. PHI must not be posted on Social Media sites such as, but not limited to, Facebook, Instagram, Snap Chat or Twitter. Personnel will be educated that simply because a patient's name is not used, does not mean that the patient or member is not identifiable.

5. Audits. Access to electronic PHI and related user activity will be periodically audited.

C. Physical Safeguards

1. Facility Security Plan.

(a) All hardware, network connections, software, data or other files will, as much as possible, will be stored away from potential natural physical hazards, such as water/cooling/heating pipes, vents or ducts, any visible signs of water/cooling/heating or other natural damage, direct sunlight, and extreme cold.

(b) Electrical circuits will not be overloaded. Additional circuits will be installed if needed. Power strips may be used where necessary, but must be used individually and not plugged into each other. VNS Health will assure that there are no frayed or otherwise defective electrical cords. Electrical equipment with cords found defective will be taken out of service promptly and replaced.

(c) Please also refer to the I.T. Access Control Policy, 7. Physical Access.

2. Access Control and Validation Procedures.

(a) Personnel will take reasonable steps to ensure that visitors do not obtain unauthorized access (e.g., question visitors who appear to be where they should not be and report any unauthorized access to Director of Safety and Security). Any person performing physical work on the premises (e.g., repair of equipment or utilities) must show identification before entering VNS Health.

(b) All Personnel must have their VNS Health -issued ID while on VNS Health's premises. Personnel must only physically access these areas containing PHI if they have a legitimate clinical or business purpose.

3. Additional Physical Safeguards. In addition to the physical safeguards discussed above, Personnel will comply with following safeguards:

(a) PHI will be securely stored in locked drawers, file cabinets, offices, or office suites when the work area is unattended.

(b) Only a patient/member first name and last initial will be posted on boards that may be viewable to the public.

(c) PHI will not be left unattended in public or other open areas, such as conference or meeting rooms.

(d) If a patient record containing PHI is placed in a bin or mailbox outside an area that is visible to visitors or others, the record will be positioned so that the PHI is not exposed.

D. Training

All Personnel will receive training at the time of employment with annual updates thereafter, or as otherwise needed, regarding VNS Health's HIPAA compliance program and the safeguards discussed in this Policy.

REFERENCES: 45 CFR §§ 164.530

Reviewed:		7/2010	9/2013	2/2014	1/2015	11/2016
Revised & Approved:	5/2009		9/2013	2/2014		11/2016
Reviewed:	4/2018	11/2019	10/2020	3/2022	6/2023	
Revised & Approved:	1/2019	1/2020	3/2021	6/2022	9/2023	