VNS HEALTH

CORPORATE POLICY & PROVIDER

TITLE: BUSINESS ASSOCIATES

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 & Legal Department

FIRST ISSUED: December 2018

NUMBER: HIPAA.17

POLICY:

VNS Health recognizes that from time to time it enters into arrangements with third parties to perform certain services for which receipt of protected health information ("PHI") may be necessary.

Except as otherwise provided herein, it is the policy of VNS Health to require that all Business Associates (as defined below) sign a business associate agreement ("BAA") which requires, among other things, the Business Associate to implement safeguards to protect electronic PHI. On a case by case basis, VNS Health will determine if additional diligence is required to ensure implementation of such safeguards.

VNS Health further recognizes that it may act as a vendor or subcontractor to another Covered Entity (e.g., providing billing services, acting as a care manager). In such cases, VNS Health will enter into a BAA with the Covered Entity.

A "**Business Associate**" is an entity that performs a service on behalf of VNS Health and receives or creates PHI in order to perform that service. When VNS Health is, itself, acting as a Business Associate, VNS Health's subcontractors that assist VNS Health in performing its Business Associate responsibilities are also Business Associates.

Business Associates do not include:

- Providers that only perform treatment services on behalf of VNS Health;
- Entities that have only incidental disclosure exposure to PHI (e.g., housekeeping, maintenance); and
- Entities that only transport information (e.g., Federal Express, US Postal Service); provided, however, entities that provide electronic data transmission services and that requires access on a routine basis to PHI are Business Associates.

All other terms not defined in this Policy will have the meaning ascribed to them in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and related regulations promulgated thereunder (the "HIPAA Regulations").

A. <u>Entering into BAA</u>

1. Whenever an individual, on behalf of a VNS Health entity, intends to enter into an arrangement with a third party, the individual will review the arrangement with the Legal Department to determine if a BAA is required.

2. If it is determined that a BAA is required, the Legal Department will prepare a BAA which, at a minimum, will include the content described in the Privacy and Security Rules (45 CFR §§164.504(e), 164.514) and may include other business terms.

3. If the Business Associate requests modification of the BAA, the Legal Department will negotiate all such modifications, as necessary; provided, however, that the BAA must retain all requirements under the Privacy and Security Rules.

4. It is preferable that VNS Health's standardized form of BAA be used in all circumstances; however, from time to time a Business Associate may require use of its BAA and VNS Health is permitted to use such third party form. The Legal Department must approve all third party BAAs, and negotiate such BAAs, as necessary. Outside legal counsel may be consulted if needed, at the discretion of the Legal Department.

5. PHI should not be provided to, or created by, a Business Associate on behalf of VNS Health until the BAA has been fully executed.

6. The Corporate Administrative Services Department will maintain a copy of all BAAs.

B. **<u>Monitoring Business Associates</u>:**

1. The BAA requires Business Associates to commit to implementing the technical, physical and administrative security features required under the Security Rule.

2. If at any time, a Business Associate reports that the Business Associate has had a Breach of Unsecured PHI, the Chief Compliance and Privacy Officer ("Privacy Officer") will, in addition to all other Breach requirements, obtain an explanation of the steps that the Business Associate is taking to prevent against similar future Breaches. The Breach and the explanation may be considered in determining the ongoing relationship with the Business Associate.

3. For any Business Associate that will be hosting VNS Health PHI, the IT Security Officer will be informed of the relationship and will determine if additional due diligence of the security of the Business Associate is necessary. Such additional due diligence may include without limitation: (a) written confirmation that a risk analysis and risk management plan has been completed, when it was performed and updated, and by whom; (b) submitting to a full security assessment to be performed by VNS Health or a commissioned third party; (c) completion of a security questionnaire; (d) providing security architecture and data flow diagrams; (e) ensuring compliance with SOC 2 Type II, HITRUST or other recognized certification standard; and/or (f) providing reports of remediation following penetration and vulnerability testing.

5. In the event that an IT Security Officer determines that a Business Associate requires additional monitoring because of the amount or sensitivity of PHI that the Business Associate will access, maintain, create or receive, the IT Security Officer will identify if any additional security measures should apply.

6. Any Business Associate that requires access to VNS Health's computer systems in order to access PHI will be subject to oversight and monitoring in accordance with procedures established by IT Security. Additionally, Business Associates will also complete, on an annual basis, all required VNS Health compliance and HIPAA training or, in the alternative, provide a signed attestation that its employees have completed annual compliance and HIPAA training that is substantially similar to training provided by VNS Health.

Reviewed & Revised:	12/2018 (New)	11/2019	10/2020	3/2022	6/2023	
Approved:	1/2019	1/2020	3/2021	6/2022	9/2023	