

## VNS HEALTH CORPORATE POLICY & PROCEDURE

**TITLE:** De-Identifying and Re-Identifying Patient/Member Health Information and Creation of Limited Data Sets

**APPLIES TO:** VNS Health Home Care, including the Home Care, and Care Management Organization (CMO) divisions;  
VNS Health Behavioral Health, Inc.;  
VNS Health Personal Care;  
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:** August 9, 2005

**NUMBER:** HIPAA.4

---

### **PURPOSE:**

VNS Health is required by law to maintain the confidentiality and privacy of a patient’s and/or member’s identifiable health information. This policy and procedure explains how VNS Health determines whether a patient’s and/or member’s health information is (i) identifiable and required to be protected or (ii) is sufficiently de-identified so that it is not subject to the confidentiality and privacy rules. This Policy also explains the circumstances pursuant to which de-identified health information may be re-identified by VNS Health. Finally, this Policy and Procedure explains: (i) the method by which a limited data set of patient or member health information can be created and (ii) the circumstances under which limited data sets can be used and disclosed for clinical research, public health and health care operations purposes.

### **POLICY:**

#### **I. DE-IDENTIFIED HEALTH INFORMATION**

A. All patient and/or member identifiable health information which has been “de-identified” (as described below) can be used or disclosed without complying with HIPAA. Health information is considered de-identified information if it does not directly or indirectly identify a patient and/or member. For information to be considered de-identified it must satisfy all of the requirements of either B(1) or B(2), below.

B. Any individual or department wishing to create or utilize de-identified information must contact the Chief Compliance and Privacy Officer (“Privacy Officer”) or the Legal

Department, who/which will ensure one of the two following HIPAA-compliant de-identification methodologies is properly followed.

1. A person or entity with appropriate knowledge of generally accepted statistical and scientific principles and methods for rendering information anonymous is engaged to determine that (a) the risk is very small that the information could be used (alone or in combination with other reasonably available information) by an anticipated recipient to identify an individual, and

(b) documents the basis for such determination.

2. All of the following identifiers of the individual and relatives, employers, or household members of the individual, have been properly removed from the information:

- (a) Names;
- (b) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, (except for the initial three digits of a zip code if the geographic unit formed by such three digits contains more than 20,000 people);
- (c) *Except for calendar years*, all dates related to an individual such as birth date, admission date, discharge date, date of death; provided however, that all individuals over 89 years of age may only be aggregated into a single category of age 90 or older and may not be categorized by calendar year;
- (d) Telephone numbers;
- (e) Fax numbers;
- (f) Electronic mail addresses;
- (g) Social security numbers;
- (h) Medical record numbers;
- (i) Health plan beneficiary numbers;
- (j) Account numbers;
- (k) Certificate/license numbers;
- (l) Vehicle identifiers and serial numbers, including license plate numbers;
- (m) Device identifiers and serial numbers;
- (n) Web Universal Resource Locators (URLs);

- (o) Internet Protocol (IP) address numbers;
- (p) Biometric identifiers, including finger and voice prints;
- (q) Full face photographic images and any comparable images; and
- (r) Any other unique identifying number, characteristic, or code (excluding the re-identification code described in III below).

VNS Health requires any information de-identified in this manner is approved by the Privacy Officer or designee prior to use or disclosure.

## **II. RE-IDENTIFYING DE-IDENTIFIED HEALTH INFORMATION**

A. VNS Health may, at its discretion, decode or translate de-identified health information in order to re-identify the information with respect to a specific individual. Before any information is de-identified, the Privacy Officer will determine whether a re-identification code is necessary. In creating a re-identification code, the following requirements must be met:

1. The re-identification process must be performed in a secure manner so that no one other than the appropriate VNS Health employee or department can re-identify such information;
2. The code, algorithm, table or other tool for re-identification may not be disclosed to any third-party or used for any purpose other than re-identification by VNS Health; and
3. The re-identification process utilized must be incapable of being translated or decoded by a third-party so as to identify the individual (e.g., the code cannot be a derivative of the individual's name).

VNS Health requires that any re-identification code is approved by the Privacy Officer prior to use or disclosure. Prior to re-identification of any information, a proper plan must be developed to ensure HIPAA-compliant protection of information subsequent to re-identification.

## **III. LIMITED DATA SETS**

A. Limited data sets of protected health information may only be used and disclosed for clinical research, public health, and health care operations purposes. Each limited data set must exclude all of the identifiers listed in (IV)(B) below and may only be disclosed after obtaining from the recipient a data use agreement as described in (V) below.

B. A limited data set is a set of protected health information from which all of the following direct identifiers of the individual and relatives, employers, or household members of the individual have been removed:

1. Names;
2. Postal address information, other than town or city, State, and zip code;

3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

C. All VNS Health individuals who wish to create a limited data set must notify the Privacy Officer, who will work with the individual to ensure one of the following is accomplished:

1. The individual properly removes all the identifiers listed in (B) above from the PHI; or
2. The individual hires a Covered Entity, an approved outside entity which VNS Health has entered into a business associate agreement, to create the limited data set.

#### **IV. DATA USE AGREEMENT**

A. Prior to disclosing a limited data set (created in compliance with the provisions of (IV) above) to any recipient, a data use agreement must be obtained from the intended recipient. The data use agreement will list the purposes for which the recipient of the limited data set can use the patient or member information and provide VNS Health with satisfactory assurance that the recipient of the limited data set will only use or disclose the patient or member information for the purposes listed.

B. Each data use agreement must contain the following:

1. A statement indicating whether the limited data set was created for research, public health or health care operations;
2. A statement of the purposes for which the recipient can use or disclose the patient or member information being provided in the limited data set. These purposes must be consistent with the reason the data use set was originally created;
3. A list of the names of all individuals or entities being provided permission to receive the limited data set under the data use agreement;
4. A statement that the recipient agrees not to use or further disclose the information in the limited data set other than as agreed to in the data use agreement or as required by the law;
5. A statement that the recipient agrees to use appropriate safeguards to prevent the use or disclosure of the patient/member information in the limited data set in any manner other than as agreed to in the data use agreement;
6. A statement that the recipient agrees to report to VNS Health if it becomes aware of any use or disclosure of the patient information in the limited data set outside of the agreed upon uses in the limited data set;
7. A statement that the recipient agrees to ensure any agents, including any subcontractors, who it provides the limited data set to will follow the same restrictions and conditions with respect to the use, disclosure and protection of the data use set;
8. A statement that the recipient agrees to not identify the information in the limited data set or attempt to contact the individuals; and
9. A statement that VNS Health can terminate the data use agreement and use of the limited data set by the recipient if it becomes aware of any pattern of behavior or activity or practice of the recipient which materially breaches or violates the data use agreement. The statement should further indicate VNS Health will report any such breach or violation to the required state and federal government agencies.

C. All data use agreements must be approved by the Legal Department prior to execution and disclosure of the related limited data set. An example of a Data Use Agreement is attached in Exhibit A.

D. VNS Health requires the individual continue to comply with VNS Health's minimum necessary policies, procedures and requirements in using and disclosing the patient information included in the limited data set.

**REFERENCES:** 45 CFR § 164.502(D); 45 CFR § 164.514(A)-(C) & (E).

<b>Reviewed:</b>		11/2007	9/2013	1/2015	11/2016	4/2018	10/2019
<b>Revised &amp; Approved:</b>	8/2005	11/2007	9/2013		11/2016	1/2019	1/2020
<b>Reviewed:</b>	10/2020	3/2022	6/2023				
<b>Revised &amp; Approved:</b>	3/2021	6/2022	9/2023				

## EXHIBIT A

### FORM OF DATA USE AGREEMENT

This Data Use Agreement, dated as of \_\_\_\_\_, 20\_\_\_\_ (“Agreement”), is by and between \_\_\_\_\_ (“Covered Entity”) and \_\_\_\_\_ (“Recipient”).

WHEREAS, Covered Entity has created a Limited Data Set which contains Protected Health Information in full compliance with the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (“HIPAA”) and related regulations promulgated by the Secretary (“HIPAA Regulations”) and specifically 45 CFR § 164.514(e).

WHEREAS, Recipient desires to use and/or disclose the Protected Health Information in the Limited Data Set which was created by VNS Health and is subject to protection under the HIPAA Regulations.

WHEREAS, in light of the foregoing and the requirements of the HIPAA Regulations, Recipient and Covered Entity agree to be bound by the following terms and conditions:

1. Definitions. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E (“Privacy Rule”).

(a) Protected Health Information. “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR 160.103, limited to the information created or received by Recipient from Covered Entity as part of the Limited Data Set.

(b) Required By Law. “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR 164.103.

2. Use and Disclosure.

(a) Purpose. Recipient agrees to not use or disclose the Protected Health Information in the Limited Data Set for purposes other than research, public health or health care operations **[Indicate Correct Purpose]** and specifically only with respect to \_\_\_\_\_.

**[Indicate Intended Use]** The Recipient has requested inclusion of and will only utilize the following elements in the Limited Data Set: \_\_\_\_\_.

**[Indicate Specific Data Elements or Categories of Data Elements]** Recipient further agrees not to use or disclose the Limited Data Set other than as permitted or required by this Agreement or as Required by Law.

(b) Limitation. Except as otherwise limited in this Agreement, Recipient may use or disclose the Limited Data Set to perform functions, activities, or services in connection with its research, public health or health care operations function **[Indicate Correct Function]**, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of VNS Health.

3. Authorized Users. The Limited Data Set must only be used or disclosed by entities or persons authorized under the Agreement. Recipient represents and warrants the following is a list of the persons within the Recipient's organization that are authorized to use or disclose the Limited Data Set: \_\_\_\_\_

4. Agents. Recipient agrees to ensure that any agent, including a subcontractor, to whom it provides the Limited Data Set, agrees to the same restrictions and conditions that apply through this Agreement with the Recipient with respect to such information. Recipient further agrees that each agent will enter into a Data Use Agreement substantially similar to this Agreement.

5. Appropriate Safeguards. Recipient agrees to use appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided for in this Agreement. Without limiting the generality of the foregoing, Recipient agrees to protect the integrity and confidentiality of any Protected Health Information it electronically exchanges with Covered Entity.

6. Reporting. Recipient agrees to report to Covered Entity any use or disclosure of the Limited Data Set not provided for by this Agreement of which it becomes aware.

7. Protection of Individuals. The Recipient agrees that it will neither identify any of the Protected Health Information provided to it in the Limited Data Set nor attempt to contact the individuals whose Protected Health Information is included in the Limited Data Set.

8. Permissible Requests by Covered Entity. Covered Entity shall not request Recipient to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule.

9. Term and Termination.

(a) Term. This Agreement shall be effective as of the date set forth above, and shall terminate when all of the Limited Data Set provided by Covered Entity to Recipient, or created or received by Recipient on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the Limited Data Set, protections are extended to such information, in accordance with the termination provisions in this section.

(b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Recipient, Covered Entity shall either:

(i) Provide an opportunity for Recipient to cure the breach or end the violation. If Recipient does not cure the breach or end the violation within the time



specified by Covered Entity, Covered Entity shall terminate this Agreement;

(ii) Immediately terminate this Agreement if Recipient has breached a material term of this Agreement and cure is not possible; or

(iii) If neither termination nor cure are feasible, Covered Entity shall report the violation to the appropriate state and federal agencies.

(c) Effect of Termination.

(i) Except as provided in paragraph (ii) of this Section 9(c), upon termination of this Agreement, for any reason, Recipient shall return or destroy the Limited Data Set and all Protected Health Information received from Covered Entity, or created or received by Recipient on behalf of Covered Entity. This provision shall apply to Protected Health Information in the possession of subcontractors or agents of Recipient. Recipient shall retain no copies of the Limited Data Set or any other Protected Health Information.

(ii) If the Recipient determines returning or destroying the Limited Data Set and the Protected Health Information is infeasible, Recipient will provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of the Limited Data Set and Protected Health Information is infeasible, Recipient will extend the protections of this Agreement to such Limited Data Set and all Protected Health Information and limit further uses and disclosures of such Limited Data Set and all Protected Health Information included therein to those purposes that make the return or destruction infeasible, for so long as Recipient maintains such Limited Data Set.

10. Miscellaneous.

(a) Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended.

(b) Amendment. The Parties agree to take such action to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and HIPAA.

(c) Interpretation. Any ambiguity in this Agreement must be resolved to permit Covered Entity to comply with the Privacy Rule.

(d) Miscellaneous. This Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein.



**IN WITNESS THEREOF**, the parties have executed this Agreement as of the date set forth above:

**[INSERT NAME OF COVERED ENTITY]**

**[INSERT NAME OF RECIPIENT]**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name:

Name:

Title:

Title: