
SUBJECT: LIMITED DATA SET

GENERAL STANDARD (PRIVACY RULE SECTION 164.514(e)):

AHS health care providers and health plans may use or disclose a limited data set if AHS enters into a data use agreement with the recipient of the limited data that meets the requirements of the Privacy Rule.

AHS health care providers and health plans may use or disclose a limited data set only for the purposes of research, public health and health care operations.

AHS health care providers and health plans will utilize a form data use agreement that will provide that the limited data set recipient will maintain the confidentiality of the information it receives and only use and disclose such information for the purposes for which such information was provided.

PRIVACY RULE:

I. Requirements for Limited Data Set

- A. A limited data set is PHI that excludes the following direct identifiers of the individual or relatives, employers or household members of the individual:
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.

II. Permitted Uses and Disclosures of Limited Data Set

- A. A CE may use or disclose a limited data set only for the purposes of research, public health, or health care operations.
- B. A CE may use PHI to create a limited data set, or disclose PHI only to a business associate for such purpose, whether or not the limited data set is to be used by the CE.

III. Data Use Agreement

- A. A CE may use or disclose a limited data set only if the CE obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this Paragraph III, that the limited data set recipient will only use or disclose the PHI for limited purposes.
- B. A data use agreement between the CE and the limited data set recipient must:
 1. Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with Paragraph II above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the Privacy Rule if done by the CE;
 2. Establish who is permitted to use or receive the limited data set; and
 3. Provide that the limited data set recipient will:
 - a. Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
 - b. Use appropriate safeguards to prevent use or disclosure of the information other than as provided by the data use agreement;

- c. Report to the CE any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
 - d. Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
 - e. Not identify the information or contact the individuals.
- C. A CE is not in compliance with the Privacy Rule if the CE knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the CE took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:
- 1. Discontinued disclosure of PHI to the recipient; and
 - 2. Reported the problem to the Secretary of Health and Human Services.
- D. A CE that is a limited data set recipient and violates a data use agreement will be in noncompliance with the Privacy Rule.

GUIDELINES:

- 1. AHS health care providers and health plans understand that they can use and disclose limited data sets **only** with respect to research, public health, or health care operations activities **and** that the limited data recipient must execute an agreement restricting its use and disclosure of the limited data set.
- 2. A form Limited Data Set Agreement is set forth below. The form is offered as a model: however, AHS health care providers and health plans are free to use other form agreements that meet the requirements of the Privacy Rule, provided they first complete the review process identified in Paragraph 3 below. The attached form agreement has blanks that must be completed – AHS includes instructional information for completing the agreement, at the end of the agreement.
- 3. AHS health care providers and health plans will not enter into any Limited Data Set Agreement, whether or not based on the form below, without first obtaining the review and approval of the Assistant Attorney General or other counsel providing services to the health care providers or health plans seeking to enter into the Limited Data Set Agreement.
- 4. In most cases, AHS health care providers and health plans will create the limited data set themselves, by either removing all of the identifiers listed above from a record or creating

a record that does not contain any of the listed identifiers. However, AHS may retain a third party to create the limited data set, provided that AHS enters into a Business Associate Agreement with such third party.

5. AHS understands that it will need to enter into a Business Associate Agreement, and a Limited Data Set Agreement, in any situation where it permits a third party to create the limited data set (thus necessitating a Business Associate Agreement), and to then use that limited data set for research, public health, or health care operations activities (thus necessitating a Limited Data Set Agreement).
6. AHS has provided training to those groups who might be responsible for the development, negotiation, and execution of Limited Data Set Agreements to ensure that such groups are aware of the steps AHS must take if and when they learn of any breach of the Limited Data Set Agreement by a recipient of the limited data set. In that regard, all such persons have been trained to promptly notify the Privacy Official of any such breach, and to then work closely with the Privacy Official on the resolution of such breach. The Privacy Official will closely monitor the return or destruction of the limited data set used, created or obtained by the recipient upon termination of a Limited Data Set Agreement.

DATA USE AGREEMENT

This Data Use Agreement ("Agreement") is entered into by and between **the State of Vermont Agency of Human Services, operating by and through its [_____]** ("Covered Entity") and [_____] ("Data User"), as of [_____] ("Effective Date").

BACKGROUND INFORMATION

A. Covered Entity possesses Individually Identifiable Health Information that is protected under the Standards for the Privacy of Individually Identifiable Health Information, at 45 CFR Parts 160 and 164 (the "Privacy Rule"), promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA");

B. Data User has offered to perform certain Activities (as defined below) for Covered Entity;

C. Covered Entity wishes to disclose a Limited Data Set (as defined below) to Data User for use by Data User in performance of the Activities;

D. Covered Entity wishes to ensure that Data User will appropriately safeguard the Limited Data Set in accordance with the HIPAA Privacy Rule; and

E. Data User agrees to protect the privacy of the Limited Data Set in accordance with the terms and conditions of this Agreement and the Privacy Rule.

Covered Entity and Data User agree as follows:

1. **Definitions.** All capitalized terms in this Agreement have the meanings identified in this Agreement or the Privacy Rule. The term "Individual" includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g). All references to PHI mean Protected Health Information.

2. Obligations of Covered Entity.

a. *Limited Data Set.* Covered Entity agrees to disclose the following PHI to Data User: _____ (the "Limited Data Set"). Such Limited Data Set shall not contain any of the following identifiers of the individual who is the subject of the PHI, or of relatives, employers or household members of the individual: names; postal address

information, other than town or city, State, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

3. Obligations of Data User.

a. *Performance of Activities.* Data User may use and disclose the Limited Data Set only in connection with the performance of the **[research activities] [public health activities] [health care operations]** provided in **Exhibit A**, attached to this Agreement (the "Activities"). Data User shall limit the use or receipt of the Limited Data Set to the following individuals or classes of individuals who need the Limited Data Set for the performance of the Activities:

[_____].

b. *Nondisclosure Except As Provided In Agreement.* Data User shall not use or further disclose the Limited Data Set except as permitted or required by this Agreement.

c. *Use Or Disclosure As If Covered Entity.* Data User may not use or disclose the Limited Data Set in any manner that would violate the requirements of the Privacy Rule if Data User were a Covered Entity.

d. *Identification Of Individual.* Data User may not use the Limited Data Set to identify or contact any individual who is the subject of the PHI from which the Limited Data Set was created.

e. *Disclosures Required By Law.* Data User shall not, without the prior written consent of Covered Entity, disclose the Limited Data Set on the basis that such disclosure is required by law without notifying Covered Entity so that Covered Entity shall have an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure, Data User shall refrain from disclosing the Limited Data Set until Covered Entity has exhausted all alternatives for relief.

f. *Safeguards.* Data User shall use any and all appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided by this Agreement.

g. *Data User's Agents.* Data User shall not disclose the Limited Data Set to any agent or subcontractor of Data User except with the prior written consent of Covered Entity. Data User shall ensure that any agents, including subcontractors, to whom it provides the Limited Data Set agree in writing to be bound by the same restrictions and conditions that apply to Data User with respect to such Limited Data Set.

h. *Reporting.* Data User shall report in writing to Covered Entity any use or disclosure of the Limited Data Set in violation of this Agreement by Data User or its agents (including subcontractors). Data User shall provide such written report promptly after it becomes aware of any such use or disclosure, and shall provide Covered Entity with the information necessary for Covered Entity to investigate any such use or disclosure.

4. Material Breach, Enforcement and Termination.

a. *Term.* This Agreement shall be effective as of the Effective Date, and shall continue until it is terminated in accordance with the provisions of Section 4.c.

b. *Covered Entity's Rights of Access and Inspection.* From time to time upon reasonable notice, or upon a reasonable determination by Covered Entity that Data User has breached this Agreement, Covered Entity may inspect the facilities, systems, books and records of Data User to monitor compliance with this Agreement. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Data User's facilities, systems and procedures does not relieve Data User of its responsibility to comply with this Agreement, nor does Covered Entity's (1) failure to detect or (2) detection of, but failure to notify Data User or require Data User's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of Covered Entity's enforcement or termination rights under this Agreement.

c. *Termination.* Covered Entity may terminate this Agreement:

(1) immediately if Data User is named as a defendant in a criminal proceeding for a violation of

HIPAA or the Privacy Rule;

(2) immediately if a finding or stipulation that Data User has violated any standard or requirement of HIPAA or the Privacy Rule, or any other security or privacy laws is made in any administrative or civil proceeding in which Data User has been joined; or

(3) pursuant to Section 4.d.(3) of this Agreement.

d. *Remedies.* If Covered Entity determines that Data User has breached or violated a material term of this Agreement, Covered Entity may, at its option, pursue any and all of the following remedies:

(1) exercise any of its rights of access and inspection under Section 4.b. of this Agreement;

(2) take any other reasonable steps that Covered Entity, in its sole discretion, shall deem necessary to cure such breach or end such violation; and/or

(3) terminate this Agreement immediately.

e. *Knowledge of Non-Compliance.* Any non-compliance by Data User with this Agreement or with HIPAA or the Privacy Rule will be considered a breach or violation of a material term of this Agreement if Data User knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance.

f. *Reporting to United States Department of Health and Human Services.* If Covered Entity's efforts to cure any breach or end any violation are unsuccessful, and if termination of this Agreement is not feasible, Covered Entity shall report Data User's breach or violation to the Secretary of the United States Department of Health and Human Services, and Data User agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against Covered Entity with respect to such report(s).

g. *Return or Destruction of Records.* Upon termination of this Agreement for any reason, Data User shall return or destroy, as specified by Covered Entity, the Limited Data Set that Data User still maintains in any form, and shall retain no copies of such Limited Data Set. If Covered Entity, in its sole discretion, requires that Data User destroy the Limited Data Set, Data User shall certify to Covered Entity that the Limited Data Set has been destroyed. If return or destruction is not feasible, Data User shall inform Covered Entity of the reason it is not feasible and shall continue to extend the protections

of this Agreement to such Limited Data Set and limit further use and disclosure of such Limited Data Set to those purposes that make the return or destruction of such Limited Data Set infeasible.

h. *Injunctions.* Covered Entity and Data User agree that any violation of the provisions of this Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law, in equity, or under this Agreement, in the event of any violation by Data User of any of the provisions of this Agreement, or any explicit threat thereof, Covered Entity shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

5. **Miscellaneous Terms.**

a. *State Law.* Nothing in this Agreement shall be construed to require Data User to use or disclose the Limited Data Set without a written authorization from an individual who is a subject of the PHI from which the Limited Data Set was created, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure. Further, in addition to applicable state law, the parties shall rely on applicable federal law (e.g., HIPAA and the Privacy Rule) in construing the meaning and effect of this Agreement.

b. *Amendment.* Data User shall cooperate with Covered Entity to amend this Agreement from time to time as is necessary for Covered Entity to comply with the Privacy Rule, or any other standards promulgated under HIPAA. This Agreement may be amended or modified, and any right under this Agreement may be waived, only by a writing signed by an authorized representative of each party.

c. *No Third Party Beneficiaries.* Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than Covered Entity and Data User, and their respective successors and assigns, any rights, obligations, remedies or liabilities. Notwithstanding the foregoing, the Covered Entity in this Agreement is the Agency of

Human Services, operating by and through its [_____] Department. Covered Entity and Data User agree that the term "Covered Entity", as used in this Agreement, also means any other Department, Division or Office of the Agency of Human Services, to the extent that such other Department, Division, or Office has a relationship with Data User that would require, pursuant to the Privacy Rule, entry into an agreement of this type.

d. *Ambiguities.* Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule, or any other standards promulgated under HIPAA.

e. *Primacy.* To the extent that any provisions of this Agreement conflict with the provisions of any other agreement or understanding between the parties, this Agreement shall control with respect to the subject matter of this Agreement. Further, and notwithstanding anything to the contrary in any such other agreement or understanding, in no event shall any provision limiting Data User's liability to Covered Entity, including, but not limited to, provisions creating a cap on damages, excluding certain types of damages, limiting available remedies, or shortening a statute of limitations, present in any such other agreement or understanding, apply with respect to any breach by Data User of any term of this Agreement.

f. *Mitigation.* Data User shall mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of a Limited Data Set in violation of any provision of this Agreement.

g. *Survival.* The provisions of this Agreement that by their terms encompass continuing rights or responsibilities shall survive the expiration or termination of this Agreement. For example, the provisions of this Agreement shall continue to apply if it would be infeasible for Data User to return or destroy the Limited Data Set, as provided in Section 4.g.

h. *Entire Agreement.* This Agreement constitutes the entire agreement of the parties with respect to its subject matter, superseding all prior oral and written agreements between the parties in such respect.

IN WITNESS WHEREOF, the parties have duly executed this Agreement as of the Effective Date.

AGENCY OF HUMAN SERVICES
(By and through its _____ Department)

[INSERT NAME OF]

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Exhibit A

Instructional Information for Completing Limited Data Set Agreement

1. Introduction. Identify the name of the AHS Department entering into the agreement, the name of the data set recipient, and the effective date of the agreement.
2. Section 2a. Identify the specific limited data set at issue – be as precise as reasonably possible.
3. Section 3. This is the first reference to Exhibit A, where the specific research, public health or health care operations activities must be identified in reasonable detail. Exhibit A is also the portion of the agreement where you would likely identify other aspects of the business relationship between AHS and the data user – e.g., how much the data user would be paid, any acceptance criteria, and when the payments would issue.

In addition, within Section 3, you must specify which activities will be performed (i.e., research, public health or health care operations) and you must specify the specific individuals, or classes of individuals, who will be permitted to have access to the limited data set.

4. Section 5c. Identify the name of the AHS Department entering into the agreement.