HIPAA Data Use Agreement [1]

Revision Date: 9/12/2013

This Data Use Agreement (the "Agreement") is entered into by and between Yale University ("Covered Entity") and _____("Data User"), collectively, the "Parties", and shall be effective as of _____ (the "Agreement Effective Date").

1. **Definitions**. The parties agree that the following terms, when used in this Agreement, shall have the following meanings, and that the terms set forth below shall be deemed to be modified to reflect any changes made hereafter to such terms by law or regulation.

   - "*HIPAA*" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

   - "*HIPAA Regulations*" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164.

   - "*Covered Entity"* means a health plan, a health care clearinghouse, or a health care provider (each as defined by HIPAA and the HIPAA Regulations) who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Regulations.

   - "*Individually Identifiable Health Information*" means information that is a subset of health information, including demographic information collected from an individual, that is;

     - created or received by a health care provider, health plan, employer, or health care clearinghouse; **and**

     - relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; **and**

     - that identifies the individual; or

     - with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

   - "*Protected Health Information*" or "*PHI*" means Individually Identifiable Health Information, except that Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, records described at 20 U.S.C. § 1232g(a)(4)(B)(iv), and employment records held by a covered entity in its role as employer.

2. **Obligations of Covered Entity.**

   - *Limited Data Set.* Covered Entity agrees to share the following Protected Health Information with Data User(s): _____ (the "**Limited Data Set**").[2] Such Limited Data Set shall not contain any of the following identifiers of the individual who is the subject of the Protected Health Information, 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.**

- *Performance of Activities.* Data User may use and disclose the Limited Data Set received from Covered Entity only in connection with the performance of the [research activities] [public health activities] [health care operations] [described in Exhibit A attached to this Agreement] [described under _____ Agreement] (the "Activities").[3]

- *Permitted Access to Limited Data Set.* 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:[4]

  _____
  _____
  _____
  _____.

- *Assurances of Data User's Non-Employee Agents.* Data User shall not disclose the Limited Data Set to any non-employee 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.

- *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.

- *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 HIPAA or the HIPAA Regulations if Data User were a Covered Entity.

- *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.

- *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 reasonably available alternatives for relief.

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

- *Reporting.* Data User shall report to Covered Entity within twenty-four (24) hours of Data User becoming aware of any use or disclosure of the Limited Data Set in violation of this Agreement or applicable law.

- *Breaches of PHI.* "Breach" shall mean the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI as defined, and subject to the exceptions set forth, in 45 C.F.R. 164.402.

Data Use shall without unreasonable delay, and in any event on or before five (5) business days after its discovery by Date User, notify Yale of any incident that involves an unauthorized acquisition, access, use, or disclosure of PHI, even if Data User believes the incident will not rise to the level of a Breach. The notification shall include, to the extent possible, and shall be supplemented on an ongoing basis with: (A) the identification of all individuals whose Unsecured PHI was or is believed to have been involved, (B) all other information reasonably requested by Yale to enable Yale to perform and document a risk assessment in accordance with 45 C.F.R. Part 164 subpart D with respect to the incident to determine whether a Breach of Unsecured PHI occurred, and (C) all other information reasonably necessary to provide notice to individuals, HHS and/or the media, all in accordance with the security breach notification requirements set forth in 42 U.S.C. § 17932 and 45 C.F.R. Parts 160 & 164 subparts A, D, & E. Notwithstanding the foregoing, in Yale's sole discretion and in accordance with its directions, Data User shall conduct, or pay the costs of conducting, an investigation of any incident required to be reported under this Section 2.1(c)(ii) and shall provide and/or pay the costs of providing, the security breach notifications pursuant to the HITECH Act.

4. **Material Breach, Enforcement and Termination.**

- *Term.* This Agreement shall be effective as of the Agreement Effective Date, and shall continue until the Agreement is terminated in accordance with the provisions of Section 4.c. [or the _____ Agreement between the parties terminates].[5]

- *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. The parties' respective rights and obligations under this Section 4.b. shall survive termination of the Agreement.

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

  - immediately if Data User is named as a defendant in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

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

  - immediately, if Covered Entity determines that Data User has breached or violated a material term of this Agreement; or

  - pursuant to Section 5.b. of this Agreement.

- *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:

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

  - 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

- terminate this Agreement immediately, in accordance with Section 4.c.

- *Knowledge of Non-Compliance*. Any non-compliance by Data User with this Agreement or with HIPAA or the HIPAA Regulations automatically 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.

- *Reporting to United States Department of Health and Human Services*. If any breach or violation is not cured, 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).

- *Disposition of Records.* Upon termination of this Agreement for any reason, Data User may retain the Limited Data Set but may only use or disclose the Limited Data Set for the purposes specified in this Agreement and only in accordance with the terms of this Agreement. This section shall survive termination of this Agreement.[6]

- *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. The parties' respective rights and obligations under this Section 4.h. shall survive termination of the Agreement.

- *Indemnification.* Data User shall indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of Data User in connection with the representations, duties and obligations of Data User under this Agreement. The parties' respective rights and obligations under this Section 4.i. shall survive termination of the Agreement.

5. **Miscellaneous Terms.**

- *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.

- *Amendment.* Covered Entity and Data User agree that amendment of this Agreement may be required to ensure that Covered Entity and Data User comply with changes in state and federal laws and regulations relating to the privacy, security, and confidentiality of PHI or the Limited Data Set. Covered Entity may terminate this Agreement upon thirty (30) days written notice in the event that Data User does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with such laws and regulations.

- *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.

- *Ambiguities*. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security and

confidentiality of PHI and the Limited Data Set, including, but not limited to, HIPAA and the HIPAA Regulations.

- *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.

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

YALE UNIVERSITY ("Covered Entity")	[DATA USER] ("Data User")
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

ASSURANCE OF COMPLIANCE WITH
DATA USE AGREEMENT[7]

The following individuals are authorized to receive and use the Limited Data Set described in the Data Use Agreement for the purposes described in Section 3 of the Data Use Agreement.

By signing below, we acknowledge the restrictions on our use and disclosure of the Limited Data Set in accordance with the Data Use Agreement.

Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

[1] The primary section of the Privacy Rule governing this Agreement is 45 C.F.R. § 164.514(e) (as promulgated in 67 Fed. Reg. 53,182 (Aug. 14, 2002)).

[2] The parties should specify the protected health information that will be included in the Limited Data Set.

[3] *See* 45 C.F.R. § 164.504(e). Exhibit A should specify the research activities, public health activities, or health care operations for which Data User may use the Limited Data Set. Alternatively, the Agreement may reference the description of activities set forth in an underlying agreement. In either case, this Agreement may not authorize Data User to use or further disclose the information in a manner that would violate the requirements of HIPAA and the HIPAA Regulations if done by Covered Entity. 45 C.F.R. § 164.514(e)(4)(ii)(A). In addition, if Data User may receive certain types of sensitive information accorded special protection under state laws, Covered Entity should modify this Agreement to meet the requirements of those laws.

[4] Covered Entity and Data User should specify the individuals who are permitted to use or disclose the Limited Data Set under the Agreement. 45 C.F.R. § 164.514(e)(4)(ii)(B).

[5] Covered Entity may wish to include the bracketed language to make this Agreement terminate when an underlying agreement with Data User terminates. Covered Entity may also consider adding language to make an underlying agreement terminate when this Agreement terminates.

[6] Covered Entity may wish to instead require the return or destruction of the Limited Data Set upon termination of the Agreement. In such case, appropriate language would be: "Within ____ days of the termination of this Agreement for any reason, Data User shall return or destroy the Limited Data Set that Data User still maintains in any form, and shall retain no copies of such Limited Data Set. Upon request of Covered Entity, Data User shall certify to Covered Entity that the Limited Data Set has been destroyed."

[7] If the "Data User" signatories are not the direct data users, the data user organization may choose to have additional assurances from the direct data users.