

TITLE

Limited Data Sets and HIPAA Data Use Agreements

PURPOSE

In accordance with 45 CFR § 164.514, this guidance:

- Provides assistance and guidance to The University of Arizona (UA) regarding the creation of a Limited Data Set (LDS);
- Sets forth the appropriate review and response to requests for Limited Data Sets; and
- Provides the general requirements of a Data Use Agreement (DUA) for a use or disclosure of a Limited Data Set.

REVIEW/REVISIONS

-
- 06/2015

REFERENCES AND RELATED FORMS

-
- Capitalized terms are defined in HIPAA Privacy Program Guidance (Definitions of Key Words) and 45 CFR Parts 160 and 164
 - Please contact the HIPAA Privacy Program or Contract & Research Support (CRS) for a Data Use Agreement or if you receive a Data Use Agreement (caution: DUAs are often included in other agreements).
 - HIPAA Privacy Program Form Q (Is it PHI?)

PROCEDURES

A Covered Entity (CE) or UA Health Care Component (HCC) may use or disclose Protected Health Information (PHI), for the purpose of research, public health, and/or health care operations as part of a Limited Data Set, when a Data Use Agreement has been properly executed.

1. The HCC may use PHI to create a Limited Data Set, or may disclose PHI to a Business Associate, pursuant to an executed Business Associate Agreement, so that the Business Associate can create a Limited Data Set.
2. UA Research: UA researchers who require a LDS must first complete the Human Subjects Protection Program form, "Human Research Determination." Research on human subjects at UA is generally not a covered activity and thus, not a Health Care Component; therefore, DUAs are generally not appropriate when a researcher seeks to disclose Individually Identifiable Health Information. Please see HIPAA Privacy Program Procedures 100 and 200 for additional information about UA's status as a Hybrid Entity.
3. Responsibility of the HIPAA Privacy Program: The HIPAA Privacy Program shall periodically reevaluate the list of DUAs to determine who is using or disclosing PHI in order to assess, to the extent feasible or required:

- a. Whether the list is complete and current and
 - b. Whether the UA department, clinic, or individual has acted in compliance with the agreement.
 - c. The UA HIPAA Privacy Program will coordinate relevant (IT) Security Rule compliance with the UA Information Security Office in order to identify systems covered by the DUA.
4. Removal of Identifiers: The following identifiers for the individual and the individual's relatives, employers, or household members must be removed to create a LDS:
- a. Names (special note: in order to meet the Safe Harbor method for de-identification, the following may not be used: patient initials, first name or last name);
 - b. Postal address information other than town/city, state and zip;
 - c. Telephone numbers;
 - d. Fax numbers;
 - e. Email addresses;
 - f. Social security numbers;
 - g. Medical record numbers;
 - h. Health plan numbers;
 - i. Account numbers;
 - j. Certificate or license numbers;
 - k. Vehicle identification/serial numbers, including license plate numbers;
 - l. Device identification/serial numbers;
 - m. Web universal resource locators (URLs);
 - n. Internet protocol (IP) addresses;
 - o. Biometric identifiers, including finger and voiceprints; and
 - p. Full face photographs and comparable images.
5. Permissible Identifiers: Any PHI that excludes the 16 categories of “direct identifiers” listed immediately above (in (d)). The health information that may remain in the information disclosed may include:
- a. Dates such as admission, discharge, service, date of death; and
 - b. City, state, five digit or more zip code.

Note: it is important to note that this information is still Protected Health Information or “PHI” under HIPAA. It is not de-identified Information and is still subject to the requirements of the Privacy Regulations applicable to Limited Data Sets and PHI.

6. Data Use Agreements: A fully executed DUA must be in place between the holder of the PHI and the researcher who is the recipient of the LDS before the LDS may be obtained. The Data Use Agreement must contain satisfactory assurances that the researcher will

only use or disclose the LDS for research purposes set forth in the Data Use Agreement.

The Data Use Agreement must meet the following requirements:

- a. Establish the permitted uses or disclosures of the information by the researcher;
 - b. Establish who is permitted to use or receive the Limited Data Set;
 - c. Provide that the researcher will not use or further disclose the information other than as permitted by the agreement or required by law;
 - d. Not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule;
 - e. Provide that the researcher will use appropriate safeguards to prevent the impermissible use or disclosure of the information;
 - f. Provide that the researcher will report to the Covered Entity any impermissible use or disclosure of which it becomes aware;
 - g. Require the researcher to ensure that any agents, including a subcontractor, to whom the researcher provides the Limited Data Set agree to the same restrictions and conditions; or
 - h. Provide that the researcher will not identify the information or contact the individuals (or otherwise attempt to do so).
7. Data Use Agreement Implementation: Contracting & Research Services (CRS) will process all Data Use Agreements. Prior to the agreement being fully executed, CRS will consult with the HIPAA Privacy Program for review and approval of the DUA to ensure compliance with HIPAA requirements. The HIPAA Privacy Officer will sign the completed DUA as an acknowledgment.