CMS Limited Data Set Data Use Agreement

Policy Guide | October 23, 2026

Contents

1. Purpose
2. Background
3. Change Log
4. Definitions
5. Limited Data Set (LDS) Request Policies
    - 5.1 Request Process
    - 5.2 Available Data Files and Variables
    - 5.3 Linking to Other Data Sources
    - 5.4 Data Access
6. Appendix A: References

1. Purpose

The purpose of the Centers for Medicare & Medicaid Services (CMS) Limited Data Set (LDS) Policy Guide is to outline the policies that govern the disclosure of LDS data for research purposes. Requesting Organizations that request LDS data must also comply with the terms of the CMS LDS Data Use Agreement (DUA).

2. Background

CMS makes certain data files available to internal and external stakeholders as allowed by federal laws, regulations, and CMS policy. CMS maintains three different categories of data files: research identifiable files, LDS files, and public use files. The privacy level of the data file dictates if a DUA is needed, the request process, and the level of review required.

LDS files contain Protected Health Information (PHI), but do not contain specific direct identifiers as set forth in the HIPAA Privacy Rule at 45 C.F.R. § 164.514(e)(2). LDS files also contain controlled unclassified information (CUI). CMS LDS files are only available for research purposes and require an LDS DUA with CMS.

3. Change Log

Change	Date
Policy Creation	August 2026
Policy Update to 5.4.1	October 2026

4. Definitions

Controlled Unclassified Information (CUI): Information that federal agencies routinely generate, use, store, and share that, while not meeting the threshold for classification as national security or atomic energy information, requires some level of protection from unauthorized access and release. Types of CUI handled at CMS include: Critical Infrastructure, Financial, Law Enforcement, Legal, Privacy (including PII and PHI), Procurement and Acquisition, Proprietary Business Information, and Tax Information. See NARA's CUI Registry for a complete list: https://www.archives.gov/cui/registry/category-list.

Data Custodian: Individual who is responsible for ensuring that the environment in which the CMS data is stored complies with all applicable CMS data security requirements, including the establishment and maintenance of security arrangements to prevent unauthorized use. This individual is responsible for taking custody of CMS data unless delegated to the Data Recipient. CMS requires only one data custodian per LDS DUA.

Data Recipient: Individual under the oversight of the Data Custodian who may take possession of CMS data, if delegated by the Data Custodian.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, in accordance with OMB Memorandum M-17-12 Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017). As noted in OMB M-17-12, the term PII is necessarily broad because there are many different types of information that can be used to distinguish or trace an individual's identity.

Protected Health Information (PHI): Information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. PHI includes many common identifiers (e.g., name, address, birth date, Social Security Number). The HIPAA definition of PHI can be found at 45 C.F.R. § 160.103.

Requester: Individual authorized to sign agreements on behalf of the Requesting Organization. This person is often referred to as the "legal signatory" and accepts all terms and conditions in the LDS DUA and attests that all the information contained in the request packet is accurate.

Requesting Organization: The organization that establishes the LDS DUA with CMS.

5. Limited Data Set (LDS) Request Policies

CMS permits external entities (referred to herein as "Requesting Organization(s)") to request access to non-public CMS data in the form of LDS files for research purposes, provided the Requesting Organization complies with the policies set forth in this Section 5 and the terms and conditions set forth in the LDS DUA. The LDS DUA is the legal agreement between CMS and the Requesting Organization that documents the terms and conditions under which the CMS data may be used. Requests for Research Identifiable Files (RIF) require a separate RIF DUA with CMS.

5.1 Request Process

Requesting Organizations requesting LDS files must complete and submit a research request through the Enterprise Privacy Policy Engine (EPPE) system. Requesting Organizations can find training to assist with the EPPE request processes on the CMS LDS website.

5.1.1 Submit Research Request

Requesting Organizations must submit their research request in EPPE by utilizing the self-service workflow. This workflow will gather the necessary information to establish the LDS DUA with CMS. As part of this workflow, Requesting Organizations will upload the following documents:

7. Attachment A: LDS Request Application
8. Data Management Plan Self Attestation Questionnaire (DMP SAQ) Approval Letter (see 5.4.1 below)
9. LDS Request Order Form
10. Signature addendum, if needed (a signature addendum is only required if the Data Custodian is designating a Data Recipient to download the LDS files)

Upon submission of the request in EPPE, the Requesting Organization agrees to the terms and conditions of the LDS DUA.

5.1.2 Undergo CMS Review

CMS reviews all LDS research requests to ensure compliance with the requirements of the HIPAA Privacy Rule, the Privacy Act of 1974, other applicable federal laws and regulations, and CMS data policies. Following review of the LDS research request, CMS may request more information, approve the request, or deny the request within the EPPE system. Associated notifications will be sent to the Requesting Organization from the EPPE system.

5.1.3 Pay CMS Fees

CMS charges fees to Requesting Organizations to recoup the cost of making data available for research

purposes. These fees are based on CMS's costs and allow the agency to continue to make data available to Requesting Organizations. CMS' LDS fees are standardized, and the agency is not able to offer discounts or concessions. CMS accepts payment of fees through automated clearing house (ACH), wire transfer or pay.gov.

LDS data fees are posted at: https://www.cms.gov/data-research/files-for-order/limited-data-set-lds-files

5.1.4 Receive Data Access

Requesting Organizations only receive access to CMS LDS data once their LDS research request is approved by CMS and CMS fees are paid. Approved LDS files must be downloaded via Secure File Transfer System (SFTS) from the CMS Virtual Research Data Center (VRDC). See policy 5.4 entitled "Data Access" for additional policies to access LDS data.

5.1.5 Publish Research

Requesting Organizations are required to publicly disseminate their research findings in compliance with the LDS DUA. CMS does not specify the mechanism for publication; Requesting Organizations may publish in peer-reviewed journals or other public forums (e.g., blog, white paper); however, the dissemination of findings should be available to the public. LDS Requesting Organizations are permitted to produce products or tools that adhere to the LDS DUA terms and conditions provided this work is secondary to the research.

5.1.6 Extend LDS DUA

CMS LDS DUAs are only approved for up to a period of one year. Requesting Organizations may request to extend their DUA by submitting an LDS DUA Extension request directly in EPPE and uploading the DUA Extension form. LDS DUA extensions can only be submitted up to 60 calendar days prior to the LDS DUA expiration date.

Requesting Organizations can request to extend their LDS DUAs for up to one year at a time. CMS will only approve extension requests if the research study is ongoing.

If a Requesting Organization does not submit a request to extend their LDS DUA within 30 days of the DUA expiration date, the organization must close the LDS DUA and destroy all LDS files.

5.1.7 Amend LDS DUA

Requesting Organizations must notify CMS of any updates or changes to their approved LDS DUA or project information by submitting an amendment request in EPPE.

5.1.8 Close LDS DUA

Requesting Organizations are required to close their LDS DUA by either the LDS DUA expiration date or

at the completion of their research project, whichever occurs first.

LDS DUAs that are not closed within 30 days of the LDS DUA expiration date are in violation of the terms of the LDS DUA. Requesting Organizations with an expired LDS DUA will be unauthorized and will not be permitted to update or extend current LDS DUAs or enter into a new LDS DUA with CMS until the violation is resolved.

5.2 Available Data Files and Variables

While CMS collects and generates a significant amount of data in running its programs, only select data files and variables are available for research purposes. CMS has developed a standard set of LDS files with defined layouts and time periods for disclosure for research purposes. CMS does not develop custom LDS files, file layouts, or data time periods. In addition, Requesting Organizations cannot request future years of data files that are not yet available. The list of data files years/quarters available to LDS Requesting Organizations may be found in the LDS Request Order Form.

5.3 Linking to Other Data Sources

CMS must approve all data linkages between LDS files and other data sources. Researchers may request linkages with a description of the linkage methodology to other data as part of the researcher's request in the LDS DUA application.

5.4 Data Access

5.4.1 Physical Data Access Requirements

CMS only makes LDS files available via download from the Chronic Conditions Warehouse Virtual Research Data Center (CCW VRDC). Requesting Organizations must list the individual(s) who will access the CCW VRDC to download data on the LDS DUA as either a Data Custodian or a Data Recipient. Up to two individuals are permitted to access the CCW VRDC to download the data for each LDS DUA. The Data Custodian/Data Recipient will be notified via email once the LDS files have been loaded into the CCW VRDC. Data is available for download from the CCW VRDC for 90 days from the date CMS loads the data file(s) into the CCW VRDC. Data must be downloaded and any issues with the data must be reported to CMS within 90 days. After 90 days, the data are archived in CMS systems and the Requesting Organization will be assessed 50% of the original fee to reload the data to the CCW VRDC. Reloading the data is only available for 9 months after the original data load date. After 9 months, the Requesting Organization must repurchase the data at full price.

The Requesting Organization must have an approved Data Management Plan Self-Attestation Questionnaire (DMP SAQ) prior to the Requesting Organization submitting a research request via EPPE. The DMP SAQ documents the organization's security and privacy controls to protect physical copies of CMS data. Requesting Organizations must submit a copy of the DMP SAQ approval letter in EPPE.

The encrypted LDS files must not be decrypted until they are loaded and fully housed within the

approved DMP SAQ environment. CMS does not allow any other transfers of the LDS files. Requesting Organizations may not store copies of the LDS files outside the boundaries of the DMP SAQ environment; the original downloaded data files must be destroyed if not downloaded directly to the DMP SAQ approved environment. See the CMS Research Data Protection Policy Guide for more information.

5.4.2 Physical Data Access Reuse Restrictions

Requesting Organizations are permitted to "reuse" physical copies of CMS data held by their organization for other research studies by submitting a new LDS request in EPPE and receiving approval from CMS. Reuse requests must comply with the LDS DUA requirements and all policies described herein.

5.4.3 Restrictions for Researchers Outside the United States

Researchers accessing LDS files must be physically located in the United States (50 states, Washington, D.C., and the territories). The individual downloading data from the CMS VRDC must be a United States citizen due to the requirement to identity proof the individual requesting access to the CCW VRDC. Requesting Organizations must store the LDS files in a system based in the United States.

6. Appendix A: References

- Requesting Limited Data Set Files web page
- Research Identifiable File Data User Agreement Policies
- HIPAA Privacy Rule 45 CFR 164.514(b)
- Certificate of Disposition (COD)
- Data Management Plan Self-Attestation Questionnaire (DMP SAQ) web page
- Health and Human Services Policy for Records Management- 6.1.2.4.1