

**INSTRUCTIONS FOR COMPLETING THE
Medicaid Agency DATA USE AGREEMENT (DUA) FORM CMS-R-0235M**

FOR USE OF CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) DATA CONTAINING INDIVIDUAL IDENTIFIERS

This agreement must be executed prior to the disclosure of data from a CMS Systems of Records containing personally identifiable information (PII) to ensure that the disclosure will comply and the data will be protected in accordance with the requirements of the Privacy Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, the Federal Information Security Management Act of 2002 (FISMA) and CMS data release policies.

This DUA is required for a State Medicaid Agency to receive LTC/MDS data deriving from Medicare and private pay residents, and must be completed prior to the release of these files to the Medicaid Agency. No DUA is needed for release of LTC/MDS data derived exclusively from Medicaid residents; however, see the section 5 instructions below. Note that all data releases to the Medicaid Agency, including releases for Medicaid-only residents, must be electronically tracked for purposes of HIPAA compliance.

Medicaid Agencies must remain aware that the use of all the MDS data, regardless of program source, is limited to the purpose indicated in section 4 below, i.e., for Medicaid program use. In addition, Medicaid Agencies must abide by all the restrictions regarding the MDS data, regardless of source, that are based on the Privacy Act and other laws and regulations and as expressed throughout this DUA.

Note:

- 1) The language contained in this agreement may not be altered in any form.**
- 2) This section intentionally left blank for Medicaid Agency DUAs.
- 3) This section intentionally left blank for Medicaid Agency DUAs.

Section #1, enter the name of the State.

Section #4, is pre-filled for Medicaid Agency DUAs. The wording is general and covers all MDS data. This all-inclusive language will reliably guide the technical staff who must retrieve the data.

Section #5, is pre-filled for Medicaid Agency DUAs. The Medicaid Agency may choose the time period for which it wishes to receive data, from a point in the past through up to 10 years into the future (see section 6 discussion of retention date). Examples are: "1998-2000"; "2001"; or "From 1998 through [insert date 10 years into the future]".

Section #6, is pre-filled for Medicaid Agency DUAs. The group of data files indicated in section 5 may be retained by the Medicaid Agency for a period of 10 years after the approval date (established by CMS) of the DUA. This date, which is 10 years in the future, is called the retention date. For cases in which the Medicaid Agency receives data in an ongoing manner, the retention date does not move forward with each data release. For example, data released two months prior to the retention date (9 years and 10 months after the DUA approval date) may only be kept by the Medicaid Agency for two months. If it wishes to continue receiving data beyond the 10 year point, the Medicaid Agency must contact CMS at least 90 days prior to the retention date to request another DUA covering the period following the 10 year retention date.

Section #16, is to be completed by the Requestor (State Medicaid Agency Representative).

Section #17, is to be completed by the Custodian, defined as that person who will have actual possession of and responsibility for the data files. **This section must be completed even if the Custodian and Requestor are the same individual.** This will typically be the manager of the Medicaid Agency unit with responsibility for the data files. If there will be additional Custodians who are not direct Medicaid Agency employees, such as academic or other consulting contractors, who assist the Medicaid Agency in its use of the data for the purposes indicated in section 4, an appropriate lead or managerial person from each such organization must complete and sign a DUA Addendum Form-CMS-R-0235a. Additional Custodians may be included as necessary over the life of the primary DUA. To include a new Custodian under an existing Medicaid Agency DUA, submit a signed DUA Addendum Form-CMS-R-0235a to the CMS Regional Office.

Section #18, is pre-filled for Medicaid Agency DUAs.

Section #19, This section intentionally left blank for Medicaid Agency DUAs .

Section #20, shall be completed by a CMS representative.

Attachment A is intentionally not required for Medicaid Agency DUAs.

Addendum, CMS-R-0235A, shall be completed when additional custodians will be accessing CMS PII data.

Once the DUA is received and reviewed for privacy and policy issues, a completed and signed copy will be sent to the Requestor and CMS or Federal Project Officer, if applicable, for their files.

Medicaid Agency DATA USE AGREEMENT
for the use of Centers for Medicare & Medicaid Services (CMS) Data Containing Individual Identifiers

DUA #

1. **PURPOSE:** In order to secure data that resides in a CMS Privacy Act System of Records (SOR), and to ensure the confidentiality, integrity and availability of information maintained by CMS, and to permit appropriate disclosure and use of such data as permitted by law, this Agreement is by and between the Centers for Medicare & Medicaid Services (CMS), a component of the U.S. Department of Health and Human Services (DHHS), and the State of _____, Agency/Department/Division _____,

hereinafter termed "User." CMS agrees to provide the User with data that reside in a CMS Privacy Act SOR as identified in this Agreement. In exchange, the User agrees to:

- a) use the data only for purposes that support the User's project or study referenced in this Agreement, which has been determined by CMS to provide assistance to CMS in monitoring, managing and improving the Medicare and Medicaid programs or the services provided to beneficiaries;
- b) ensure the integrity and confidentiality of the data by complying with the terms of this Agreement and applicable law, including the Privacy Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act of 2002 (FISMA); and
- c) this section intentionally left blank for Medicaid Agency DUAs.

2. **CONDITIONS:** This Agreement addresses the conditions under which CMS will disclose and the User will obtain, use, reuse and disclose the CMS data file(s) specified herein, and/or any derivative file(s) that contain direct individual identifiers or elements that could be used in concert with other information to identify individuals. This Agreement supersedes any and all agreements between the parties with respect to the use of data from the file(s) specified herein and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any grant award or other prior communication from the Department of Health and Human Services (DHHS) or any of its components with respect to the data specified herein. Further, the terms of this Agreement may be changed only by a written modification to this Agreement or by the parties adopting a new agreement. The parties agree further that instructions or interpretations issued to the User concerning this Agreement or the data specified herein, shall not be valid unless issued in writing by the CMS signatory in section 20 below. The parties agree further that CMS makes no representation or warranty, either implied or expressed, with respect to the accuracy of any data in the file(s).

3. **OWNERSHIP RIGHTS:** The parties mutually agree that CMS retains all ownership rights to the data file(s) referred to in this Agreement, and that the User does not obtain any right, title, or interest in any of the data furnished by CMS.

4. **PROJECT IDENTIFICATION:** The User represents, and in furnishing the data file(s) specified in section 5 below, CMS relies upon such representation, that such data file(s) will be used solely for the following purpose(s).

Medicaid Long Term Care Minimum Data Set (LTC/MDS)

To facilitate the administration of a Federal health program for the purposes of determining participation requirements, evaluating and and/or assessing cost effectiveness, and/or the quality of health care services provided, and/or for setting long term care Nursing Facility reimbursement rates in the State that are directly related to the administration of the State Medicaid Program and to facilitate State compliance with the requirements of the Americans with Disabilities Act.

Research Users must provide a summary explanation of the research project using the template in Attachment A which is incorporated by reference into this Agreement. Only direct CMS contractors and States are exempt from the Attachment A requirement to this Agreement.

The User represents further that, except as specified in an Enclosure to this Agreement or except as CMS shall authorize in writing, the User shall not reuse, disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person(s) or organization(s). The User affirms that the requested data is the minimum necessary to achieve the purposes stated in this section. The User agrees that, within the User's organization, access to the data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this section and only to those individuals on a need-to-know basis. Disclosure of this data is made pursuant to:

- Privacy Act of 1974 5 U.S.C. Section 552a as amended;
- Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503);
- Freedom of Information Act 5 U.S.C. Section 552 as amended by P.L. 104-231, 110 Stat. 3048;
- Section 1106 of the Social Security Act (42 U.S.C. Section 1306);
- Section 1843 of the Social Security Act (42 U.S.C. Section 1395v); and
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 C.F.R. Parts 160 and 164).

The User represents further that the facts and statements made in any study or research protocol or project plan(s) submitted to CMS for each purpose are complete and accurate. Further, the User represents that said study protocol(s) or project plan(s) that have been approved by CMS or other appropriate entity as CMS may determine, represent the total use(s) to which the data file(s) specified in section 5 below will be put.

5. **DATA DESCRIPTION:** The following CMS data file(s) is/are covered under this Agreement.

File	Years(s)
LTC/MDS Resident Assessment Data Files (s)	

6. **EXPIRATION DATE:** The parties mutually agree that the aforesaid files(s) and/or any derivative file(s), including those files that directly identify individuals or maintains continued identification of individuals, may be retained by the User **for a maximum period of ten (10) years from the effective date of this agreement**, hereinafter known as the "Expiration Date." The User agrees to provide CMS, within 15 days of the completion of the purpose specified in section 4 above, but no later than the expiration date, as amended, in the method prescribed by CMS, a certification of the disposition of all the data as specified in section 5 above and as applicable all derivative files. The User agrees that no data from CMS records, or any parts thereof, shall be retained when the aforementioned certification has been provided to

CMS. The User acknowledges that stringent adherence to the aforementioned information outlined in this paragraph is required. The User acknowledges that the date is not contingent upon action by CMS.

The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Immediately, upon notice of termination by the User, CMS will cease releasing data from the file(s) to the User under this Agreement and will notify the User to destroy such data file(s). Sections 3, 4, 6, 8, 9, 10, 11, 13, 14 and 15 shall survive termination of this Agreement.

7. DATA PROTECTION: The User agrees to establish appropriate management, operation and technical controls to protect the confidentiality, integrity and availability of the data and to prevent unauthorized use or disclosure. The safeguards shall provide a level and scope of security that is not less than the level and scope of protection as established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems, http://www.whitehouse.gov/omb/circulars_a130, as well as Federal Information Processing Standard 200, "Minimum Security Requirements for Federal Information and Information Systems", <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>, and National Institute of Science and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems", <http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf>, including any revisions as applicable. The User acknowledges that the use of unsecured telecommunications, including the Internet, to transmit individually identifiable, or deducible information derived from the file(s) specified in section 5 above is prohibited. Further, the User agrees that the data must not be physically moved, transmitted or disclosed in any way from or by the site indicated in section 17 below without written approval from CMS unless such movement, transmission or disclosure is required by law.

8. SECURITY COMPLIANCE OVERSIGHT: The User agrees that the authorized representatives of CMS, the DHHS Office of the Inspector General, or the Comptroller General, will be granted access to premises where the aforesaid file(s) is/are kept for the purpose of inspecting security arrangements confirming whether or not the User is in compliance with the security requirements specified in section 7 above.

9. MINIMUM CELL SIZE DISCLOSURE: The User agrees not to disclose direct findings, listings, or information derived from the file(s) specified in section 5 above, with or without direct identifiers, if such findings, listings, or information may, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s), or date of death. The User agrees further that CMS shall be the sole judge as to whether any finding, listing, or information, or any combination of data extracted or derived from CMS' files identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual with a reasonable degree of certainty.

The User agrees that any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in section 4 above (regardless of whether the report or other writing expressly refers to such purpose, to CMS, or to the file(s) specified in section 5 or any data derived from such file(s)) must adhere to CMS' current cell size suppression policy. **This policy stipulates that no cell size (e.g. admittances, discharges, patients, services) less than 11 may be displayed.** Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell of less than 11. By signing this Agreement the User hereby agrees to abide by these rules and, therefore, will not be required to submit any written documents for CMS review. If the User is

unsure, they may submit their product to CMS for review prior to publication. CMS agrees to make a determination about approval and to notify the user within 4 to 6 weeks after receipt of findings. CMS may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual beneficiaries.

10. **RECORD LINKAGE:** The User shall not attempt to identify or contact any specific individual whose record is included in the files listed in section 5 above. The User agrees that, absent express written authorization from the CMS signatory designated in section 20 below, the User shall not attempt to link records included in the file(s) specified in section 5 above to any other individually identifiable source of information. This includes attempts to link the data to other CMS data. A protocol that includes the linkage of specific files that has been approved in accordance with section 4 above constitutes expressed authorization from CMS to link files as described in the protocol.

11. **DATA RE-USE:** The User understands and agrees that they may not reuse original or derivative data files without prior written approval from the CMS signatory in section 20 below.

12. **ENCLOSURES:** The parties mutually agree that the following specified Enclosure(s) is part of this Agreement: _____

13. **DATA BREACHES:** The User agrees that in the event CMS determines or has a reasonable belief that the User has made or may have made a use, reuse or disclosure of the aforesaid file(s) that is not authorized by this Agreement or another written authorization from the CMS signatory in section 20 below, CMS, at its sole discretion, may require the User to:

- (a) Promptly investigate and report to CMS the User's determinations regarding any alleged or actual unauthorized use, reuse or disclosure;
- (b) Promptly resolve any problems identified by the investigation;
- (c) Submit a formal response to an allegation of unauthorized use, reuse or disclosure;
- (d) Submit a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and
- (e) Return data files to CMS or destroy the data files it received from CMS under this agreement.

The User understands that as a result of CMS' determination or reasonable belief that unauthorized uses, reuses or disclosures have taken place, CMS may refuse to release further CMS data to the User for a period of time to be determined by CMS.

The User agrees to report within one (1) hour, any breach of personally identifiable information (PII) from the CMS data file(s), loss of these data or disclosure to any unauthorized persons to the CMS IT Service Desk by telephone at (410) 786-2580 or by e-mail notification at **cms_it_service_desk@cms.hhs.gov** and to cooperate fully in the federal security incident process. While CMS retains all ownership rights to the data file(s), as outlined in section 3 above, the User shall bear the cost and liability for any breaches of PII from the data file(s), or as applicable any derivative file(s), while they are entrusted to the User. Furthermore, if CMS determines that the risk of harm requires notification of affected individual persons of the security breach and/or other remedies, the User agrees to carry out these remedies without cost to CMS.

14. DISCLOSURE PENALTIES

a. The User hereby acknowledges that criminal penalties under §1106(a) of the Social Security Act (42 U.S.C. § 1306(a)), including a fine not to exceed \$10,000 or imprisonment not exceeding 5 years, or both, may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law.

b. The User further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i) (3)) may apply if it is determined that the Requestor or Custodian, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses. Any person found to have violated sec. (i)(3) of the Privacy Act shall be guilty of a misdemeanor and fined not more than \$5,000.

c. The User also acknowledges under HIPAA, "General Penalty for Failure to Comply with Requirements and Standards" Section 1176, that the DHHS Secretary may impose fines for noncompliance as high as \$100 per offense, with a maximum of \$25,000 per year on any person who violates a provision of this part; "Wrongful Disclosure of Individually Identifiable Health Information" Section 1177, that a person who knowingly:

(A) uses or caused to be used a unique health identifier;

(B) obtains individually identifiable health information relating to an individual;
or

(C) discloses individually identifiable health information to another person,

- shall be fined not more than \$50,000, imprisoned not more than 1 year, or both;
- if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and
- if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.

d. Finally, the User acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641, Protection of Government Property, if it is determined that the User, or any individual employed or affiliated therewith, has taken or converted to their own use data file(s), or received the file(s) knowing that they were stolen or converted. Under such circumstances, they shall be fined under Title 18 or imprisoned not more than 10 years, or both; but if the value of such property does not exceed the sum of \$1,000, they shall be fined under Title 18 or imprisoned not more than 1 year, or both.

15. USER AGREEMENT: By signing this Agreement, the User agrees to abide by all provisions set out in this Agreement and acknowledges having received notice of potential criminal or administrative penalties for violation of the terms of the Agreement.

16. **REQUESTOR:** The parties mutually agree that the individual identified in this section is designated as “Requestor” of the file(s) on behalf of the User and hereby attests that he or she is authorized to legally bind the User to the terms of this Agreement and agrees to all the terms specified herein. The User agrees to notify CMS, in the method prescribed by CMS, within fifteen (15) days of any change of Requestor.

Name <i>(typed or printed)</i>		Title
Company/Organization		
Street Address City	State	ZIP Code
Office Telephone <i>(Include Area Code)</i> extension (if applicable)	E-Mail Address	
Signature	Date	

17. **CUSTODIAN:** The parties mutually agree that the following named individual is designated as Custodian of the file(s) on behalf of the User and will be the person responsible for the observance of all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use or disclosure. The User agrees to notify CMS within fifteen (15) days of any change of custodianship. The parties mutually agree that CMS may disapprove the appointment of a custodian or may require the appointment of a new custodian at any time.

The Custodian hereby acknowledges his/her appointment as Custodian of the aforesaid file(s) on behalf of the User, and agrees to comply with all of the provisions of this Agreement on behalf of the User.

Name <i>(typed or printed)</i>		Title
Company/Organization		
Street Address City	State	ZIP Code
Office Telephone <i>(Include Area Code)</i> extension (if applicable)	E-Mail Address	
Signature	Date	

18. **PRIVACY ACT DISCLOSURE PROVISION:** The disclosure provision(s) that allows the discretionary release of CMS data for the purpose(s) stated in section 4 above is: (To be completed by CMS Privacy staff) Long Term Care Minimum Data set, System of Records #09-70-1517, routine use #2(c).

19. This section intentionally left blank for Medicaid Agency DUAs.

20. **CMS REPRESENTATIVE:** The parties mutually agree that the following named individual will be designated as point-of-contact for the Agreement on behalf of CMS. On behalf of CMS the undersigned individual hereby attests that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Name of CMS Representative (*typed or printed*)

A. Title/Component Street Address		Mail Stop
City	State	ZIP Code
Office Telephone (<i>Include Area Code</i>)		E-Mail Address
Signature of CMS Representative		Date
B. Concur/Nonconcur — Printed Name and component		Date
Signature of CMS Business Owner		
C. Concur/Nonconcur — Printed Name and component		Date
Signature of CMS Business Owner		
D. Concur/Nonconcur — Printed Name and component		Date
Signature of CMS Business Owner		

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0734. The time required to complete this information collection is estimated to average 20 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: Reports Clearance Officer, Baltimore, Maryland 21244-1850.