

Supporting Statement For Paperwork Reduction Act Submissions

A. Background

The Privacy Act of 1976, §552a requires the Centers for Medicare & Medicaid Services (CMS) to track all disclosures of the agency's Personally Identifiable Information (PII) and the exceptions for these data releases. CMS is also required by the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Federal Information Security Management Act (FISMA) of 2002 to properly protect all PII data maintained by the agency. Part of this protection mandates that the data be destroyed when no longer required in a manner that prevents any unauthorized disclosure. When entities request CMS PII data, they enter into a Data Use Agreement (DUA) with CMS. The DUA stipulates that the recipient of CMS PII data must properly protect the data according to FISMA and also provide for its appropriate destruction at the completion of the project/study or the expiration date of the DUA. However, under certain circumstances, the data may be approved in writing by CMS for re-use in an additional or follow-on project/study. The DUA Certificate of Disposition (COD) form provides the data recipient to document accordingly this variance in the disposition of the data or the outright destruction of the data. The "Data Use Agreement (DUA) Certificate of Disposition (COD) for Data Acquired from the Centers for Medicare & Medicaid Services (CMS)" will be used by recipients of CMS Data to certify that they have properly disposed of the data that they have received through a CMS DUA. The form requires the submitter to provide the Requestor's organization; DUA number; identification by initials as to the actual disposition of the data; listing of the data descriptions and the years of the data; printed name, phone number and e-mail address of the individual signing the form; signature and date signed; and optional point of contact name, phone number and e-mail address regarding the COD.

B. Justification

1. Need and Legal Basis

The Privacy Act of 1974 allows for discretionary releases of data maintained in Privacy Act protected systems of records under §552a(b) (Conditions of Disclosure). The mandate to account for disclosures of data under the Privacy Act is found at §552a(c)(Accounting of Certain Disclosures). This section states that certain information must be maintained regarding disclosures made by each agency. This information is: Date, Nature, Purpose, and Name/Address of Recipient. Section 552a(e) sets the overall Agency Requirements that each agency must meet in order to maintain records under the Privacy Act. The Data Use Agreement (DUA) Certificate of Disposition (COD) is required to close out the release of the data under the DUA and to ensure the data are destroyed and not used for another purpose without written authorization from CMS. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, §1173(d) (Security Standards for Health Information) requires CMS to protect Personally Identifiable Information (PII). Additionally, the Federal Information Security Management Act (FISMA) of 2002, §3544 (b) (Federal Agency Responsibilities –

Agency Program) also requires CMS to develop policies and procedures for the protection and destruction of sensitive data to include PII.

2. Information Users

The information collected by the DUA Certificate of Disposition is used by CMS to document the appropriate disposition of the data from a DUA at the completion of the project/study or DUA expiration date.

3. Use of Information Technology

DUA Certificates of Disposition may be filled in on-line and then must be printed and signed. The signed form may be submitted to CMS as a .pdf scanned document attached to an e-mail. It is estimated that 80% of all Certificates of Disposition will be submitted to CMS via e-mail attachment. CMS currently has no technology in place to support electronic signatures. When CMS has the capability to accept electronic signatures and our information system that tracks all DUAs, the Data Agreement and Data Shipping System (DADSS) has been appropriately modified, the DUA COD will be accepted with an electronic signature. It is currently unknown as to if or when CMS will implement electronic signature capabilities.

4. Duplication of Efforts

This information collection does not duplicate any other effort and the information cannot be obtained from any other source

5. Small Businesses

No special considerations are given to small businesses; however, the burden to any User/Requestor of data is minimal.

6. Less Frequent Collection

Data is collected only once at the completion of a project/study or when the expiration date for the DUA is reach. There are no additional means for reducing the data collection burden and still be compliant with statutes and CMS policy/procedures.

7. Special Circumstances

No special circumstances.

8. Federal Register/Outside Consultation

The 60-day Federal Register notice was published on April 8, 2011.

9. Payments/Gifts to Respondents

There were no payments/gifts to respondents.

10. Confidentiality

The paper DUA Certificates of Disposition are kept in filing cabinets in a locked environment. Files containing Certificates of Disposition or information from these forms will be safeguarded in accordance with Departmental standards and National Institute of Standards and Technology (NIST) Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations which limits access to only authorized personnel. The safeguards shall provide a level of security as required by Office of Management and Budget (OMB) Circular No. A-130 (revised), Appendix III – Security of Federal Automated Information Systems.

11. Sensitive Questions

There are no sensitive questions arising from this data collection.

12. Burden Estimates (Hours & Wages)

We estimate the time to complete the Certificate of Disposition is 10 minutes per requestor. We estimate that it will take 5 minutes to complete and submit the form and an additional 5 minutes to file a copy of the certificate of data destruction. On an annual basis, we expect to receive an average of 500 Certificates of Disposition for a total of 84 annual hours. We used the General Schedule (GS) 12 step 10 pay scale with locality pay adjustment for the Washington/Baltimore/Northern Virginia area as our basis for the cost burden.

Reporting Requirement

500 respondents x (5 min/60 min/hr) = 42 hours

Recordkeeping Requirement

500 respondents x (5 min/60 min/hr) = 42 hours

Cost Burden

500 requestors x \$46.64 per hour x 10 minutes each = \$3,885.11

13. Capital Costs

There are no capital costs.

14. Cost to Federal Government

It is estimated that CMS uses one full time equivalent (FTE) at the GS12 step 10 rate for an annual cost of \$97,333.

15. Changes to Burden

None

16. Publication/Tabulation Dates

There are no publication and tabulation dates associated with this collection.

17. Expiration Date

CMS would like an exemption from displaying the expiration date as these forms are used on a continuing basis. To include an expiration date would result in having to discard a potentially large number of forms.

18. Certification Statement

There are no exceptions to the certification statement.