Supporting Statement A

Data Management Plan Self-Attestation Questionnaire (DMP SAQ)
(CMS-10773, OMB 0938-New)

Background

The Privacy Act of 1974, §552a requires the Centers for Medicare & Medicaid Services (CMS) to track all disclosures of the agency's Personally Identifiable Information (PII). 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 PHI data maintained by the agency and account for the disclosure of PHI. When entities, such as academic, federal or state agency researchers or CMS contractors request CMS PII/PHI data, they enter into a **Data Use Agreement** (DUA) (OMB# 0938-0734) with CMS. The DUA stipulates that the recipient of CMS data must properly protect the data according to all applicable data security standards and also provide for its appropriate destruction at the completion of the project/study or the expiration date of the DUA.

This request is for the **Data Management Plan Self-Attestation Questionnaire (DMP SAQ)** form that will be required of DUA requesting organizations.

The CMS is permitted to disclose CMS data for research purposes to organizations that have been approved through the research data request process. To qualify to receive CMS data, requesting organizations must compile a data request packet. The data request packet's primary components are the Data Use Agreement (DUA) and the Data Management Plan Self-Attestation Questionnaire (DMP SAQ).

As per the DUA, pg. 5, the DUA legally binds the user to the Agreement's terms. The user must agree to all the terms and sign off on them prior to the release or access to data files containing protected health information, and individual identifiers. The DMP SAQ is a technical, evidence based questionnaire that DUA users must complete as part of the data request packet. The DMP SAQ will enable CMS to evaluate researcher data systems to ensure that CMS data are adequately secured and appropriately protected, as per the Privacy Act and the HIPAA Privacy Rule. The DMP SAQ also allows CMS to measure compliance through the implementation of security and privacy controls as outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-53 and the Centers for Medicare & Medicaid Services (CMS) Information Security and Acceptable Risk Safeguards (ARS). The second component of the DMP SAQ is to provide ongoing oversight. All organizations will be subject to routine audits of the environments used to store and process CMS data, as described in their organizational-level DMP SAQ.

A DMP SAQ is required each time a DUA is established. Both the DUA and the DMP SAQ forms are valid for one year from the date of approval and are renewable at expiry. If the environment

described in a DMP SAQ is the same for multiple DUAs from a single organization, the same DMP SAQ can be used across the DUAs, provided it has not expired.

A. **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) form is needed as part of the review of each CMS data request to ensure compliance with the requirements of the Privacy Act for disclosures that contain PII.

The DUA form also provides data requestors and custodians with a formal means to agree to the data protection and destruction statutory and regulatory requirements of CMS' PII data. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, §1173(d) (Security Standards for Health Information) requires CMS to protect Protected Health Information (PHI). Additionally, Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541-3549, as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283) 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 DMP SAQ form is used by CMS to conduct reviews and audits to ensure that research organization's computing environments have security and privacy controls in place to protect CMS data to comply with NIST SP 800-53, Rev. 4 and CMS ARS 3.1.

3. Use of Information Technology

The DMP SAQ form is filled out and submitted via email to the CMS Research Data Assistance Center. The form will be downloadable from the CMS website, and well as provided by the Research Data Assistance Center. The form collects organization and environment information, followed by 97 Security protection questions and 16 Privacy protection questions.
The questions in the form ensure that users of CMS data are in compliance with security and privacy controls identified by the following frameworks:

- CMS *Acceptable Risk Safeguards* (ARS),Version 3.1, and
- National Institute of Standards of Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

CMS accepts digital signatures on the form.

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 onset of the study/project and then only again if there are changes initiated by the Requestor. There are no additional means for reducing the data collection burden and still be compliant with all applicable statutory and regulatory requirements, as well as CMS policies/procedures. Yearly, the organization will attest that there are no changes via email.

7. Special Circumstances

There are no special circumstances that would require an information collection to be conducted in a manner that requires respondents to:

- Report information to the agency more often than quarterly;
- Prepare a written response to a collection of information in fewer than 30 days after receipt of it;
- Submit more than an original and two copies of any document;
- Retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years;
- Collect data in connection with a statistical survey that is not designed to produce valid and reliable results that can be generalized to the universe of study,
- Use a statistical data classification that has not been reviewed and approved by OMB;
- Include a pledge of confidentiality that is not supported by authority established in statute or regulation that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or
- Submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

8. Federal Register/Outside Consultation

The 60-day Federal Register notice published in the Federal Register 12/07/2020 (85 FR 78855).

No comments were received during the comment period.

The 30-day Federal Register notice published in the Federal Register 2/18/2021 (86 FR 10106).

Outside Consultation

A DMP SAQ pilot was conducted to test the new security and privacy requirements associated with the use of data for research purposes. Six organizations completed the pilot program. During the process, CMS solicited feedback from the participating organizations on two occasions — midway through the pilot and at the end, after each DMP SAQ was completed and submitted for review. The primary takeaway from both surveys was a need to enhance the user-friendliness. CMS took into account that the DMP SAQ form is technical and would require input from the organization's IT staff members. As a result, the form was updated to speak to an audience of both researchers and IT staff, enhance readability, streamline questions to limit redundancy, and to consolidate document requirements.

9. Payments/Gifts to Respondents

There were no payments/gifts provided to respondents for their participation or usage of the form. The DUA form is used to help CMS track disclosures, conditions for disclosure, accounting of disclosures and agency requirements.

The DMP SAQ, through the review of technical and physical safeguards in place at an organization, allows CMS to ensure that patient data is adequately protected, as per the Privacy Act, the Privacy Rule and CMS data release policies. The DMP SAQ must be completed prior to the release of, or access to, specified data files containing protected health information and individual identifiers. It also allows organizations to verify that they are using industry-level best practices and standards to secure data. As needed, the CMS contractor will provide additional guidance to researchers on implementing effective measures that protect CMS data.

10. Confidentiality

The files are maintained electronically in the Enterprise Privacy Policy Engine.

11. Sensitive Questions

There are no sensitive questions arising from this data collection.

12. Burden Estimates (Hours & Wages)

Wages

To derive average costs, we used data from the U.S. Bureau of Labor Statistics' May 2019 National Occupational Employment and Wage Estimates for all salary estimates

(http://www.bls.gov/oes/current/oes_nat.htm). In this regard, the following table presents the mean hourly wage, the cost of fringe benefits (calculated at 100 percent of salary), and the adjusted hourly wage.

Occupation Title	Occupation Code	Mean Hourly Wage ($/hr)*	Fringe Benefit ($/hr)	Adjusted Hourly Wages ($/hr)
Business Operation Specialist	13-1000	$36.31	$36.31	$72.62

As indicated, we are adjusting our employee hourly wage estimates by a factor of 100 percent. This is necessarily a rough adjustment, both because fringe benefits and overhead costs vary significantly from employer to employer, and because methods of estimating these costs vary widely from study to study. We believe that doubling the hourly wage to estimate total cost is a reasonably accurate estimation method.

Requirements and Associated Burden

a) DMP SAQ- We estimate the time to complete the DMP SAQ form is 1.5 hours. We estimate that it will take 1 hour and 25 min to complete the form and 5 min for filing. On an annual basis, we expect to receive ~1,000 DMP SAQ forms for an annual total of 1,500 hours burden.

Summary	**No. Respondents**	**Responses (per Respondent)**	**Total Responses**	**Time (per response hours)**	**Total Time (hours)**	**Labor Rate ($/hr)**	**Total Cost**
DMP SAQ	1,000	1	1,000	1.5	1,500	$72.62	$108,930

13. Capital Costs

There are no capital costs.

14. Cost to Federal Government

We use a contractor (MBL Technologies) to receive and review the DMP SAQ forms. The contractor price for intake and review is $275.00. We estimate there will be about 1,000 form submissions per year.

Task	Units	Price	Total
Intake, Completeness Review	1,000	$275.00	$275,000

In addition to reviews, our contractor (MBL Technologies) performs audits based on the DMP SAQ. These audits are broken down into three tiers based on risk.

Task	Units	Price	Total
Tier I Audit	200	$2,000.00	$400,000
Tier II Audit	80	$4,500.00	$360,000
Tier III Audit	60	$10,000.00	$600,000
		Total	$1,360,000

The cost to receive/review the DMP SAQ forms and perform audits based on the DMP SAQ equate to a total cost of $1,635,000.

15. Changes to Burden

This is a new collection.

16. Publication/Tabulation Dates

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

17. Expiration Date

The expiration date is displayed on the final page of the DMP SAQ.

18. Certification Statement

There are no exceptions to the certification statement.