September 20, 2023

Frequently Asked Questions (FAQs)

Purpose of Document

These Frequently Asked Questions (FAQs) and supporting answers are designed to assist research Data Use Agreement (DUA) requesting organizations with completing the Data Management Plan Self-Attestation Questionnaire (DMP SAQ).

Background

The Centers for Medicare and Medicaid Services (CMS) are permitted to disclose CMS data to requesting research organizations for research purposes only. As part of the disclosure process, approved requesters enter into DUAs with CMS. The DUA outlines specific requirements to ensure that the disclosure of CMS data complies with CMS data release policies and related frameworks[1].

Specifically, the DUA states: "The Requesting Organization […] ensures they adhere to the appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data set file(s) and to prevent unauthorized use or access to it…" These safeguards must be aligned with security and privacy controls identified by the following components of risk management frameworks:

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

The CMS Office of Enterprise Data Analytics (OEDA) manages the Data Privacy Safeguard Program (DPSP) to review DMP SAQs for compliance with these standards and policies.

Frequently Asked Questions

These FAQs are presented in the following categories:

Key Terms

1. **Q: What is a *DMP SAQ*?**
   A: A Data Management Plan Self-Attestation Questionnaire (DMP SAQ) is a questionnaire that a DUA requesting organization will complete for each computing environment where CMS data is processed or stored to attest that information security and data privacy requirements are in line with CMS policy and recognized data security best practices. The DMP SAQ is an organizational-level plan which means that one DMP SAQ could cover an entire organization if the organization uses a single computing environment to process and store CMS data. Instead of submitting a DMP for each study, a single DMP SAQ can be kept on file for each computing environment. The organizational-level DMP SAQ is valid for a year from the date of approval.

[1] Other relevant authorities to this Introduction include:

- Office of Management and Budget (OMB) Circular A-130, Appendix III--*Security of Federal Automated Information Systems*
- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems"*
- The Privacy Act of 1974, §552
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act (FISMA) of 2002

2. **Q: What is a *computing environment*?**
   A: A computing environment is the collection of computer components used to process and store CMS data including but not limited to servers, workstations, networking equipment, storage systems, etc. A computing environment could be onsite, leverage a Cloud Service Provider (CSP), or a hybrid.

Roles & Responsibilities

3. **Q: Who at my organization would be best suited to complete the DMP SAQ?**
   A: The individuals best suited to complete the DMP SAQ within your organization may have the title of Chief Information Security Officer (CISO), Chief Security Officer (CSO), Security Architect, Security Administrator, Data Privacy Officer, Data Security Analyst, Information Assurance Analyst, Information Security Manager, Network Security Administrator, System Administrator, Network Engineer/Administrator, etc. The individual should have a thorough understanding of the organization's security strategy, IT infrastructure, policies, procedures, and network diagram. The individual should also have a general knowledge of cybersecurity and implementing NIST controls.

4. **Q: What is a Data Custodian?**
   A: The Data Custodian is the individual responsible for the observance of all conditions of use for the environment identified in the DMP SAQ, including the establishment and maintenance of security arrangements to prevent unauthorized use. The Data Custodian will sign the final attestation statement of the DMP SAQ and will become the primary Data Custodian for each DUA associated with the DMP SAQ. DUAs will no longer list individual data users as data custodians.

Completing the DMP SAQ

5. **Q: I have been contacted by MBL Technologies. Can I talk to them about my data request?**
   A: Yes, MBL Technologies is CMS' authorized contractor responsible for reviewing your organization's DMP SAQ.

6. **Q: When should our organization answer *"Yes"* to a DMP SAQ question?**
   A: You should answer *"Yes"* once you have read the question in its entirety and can confirm through policies, procedures, and/or forms/templates, that all elements of the question have been implemented at your organization. The security control implementation will be unique to every computing environment. Rationales should explain how the control is implemented, cite policies and procedures, and explicitly address any gaps in the implementation and/or compensating controls in effect.

7. **Q: When should our organization answer "No" to a DMP SAQ question?**
   A: You should answer *"No"* once you have read the question in its entirety and can confirm through policies, and procedures that all elements of the question have not been implemented at your organization. A rationale is required for all "No" responses in both sections A and B. Rationales should explain why the control cannot be met, how your organization will remediate the missing control, and/or any compensating controls in effect.

8. **Q: Will our organization be penalized for answering "No" to any questions on the questionnaire?**
   A: Answering "No" does not automatically mean that your organization has failed the control. Please utilize the text field in the DMP SAQ to explain the following:
   a. Why the control has not been implemented.
   b. How your organization is mitigating any of the risk(s) associated with not implementing the control, and
   c. When the control will be implemented, if it is being planned for a later date.

9. **Q: What if I do not know the answer? Should I leave it blank?**
   A: Your DMP SAQ is required to be complete before the DMP SAQ can be submitted and included in your DUA request packet. Therefore, all questions will require a response. If your organization is unsure of how to respond to a question, please review the DMP SAQ guidance found on the ResDAC website, search through your organization's website for policy information, contact your organization's IT department, and/or contact your DPSP reviewer for additional guidance.

10. **Q: Does our organization need to provide any supporting documentation with the DMP SAQ?**
    A: Yes, your organization will need to provide any policies and/or procedures cited or referenced in your rationales. The DPSP may reach out to request this documentation, if needed. Supporting documentation can be linked in the DMP SAQ rationales as long as they are accessible. Please note, where rationale is required, it is not acceptable to solely cite or reference a policy, a rationale must also describe the method by which the question is being addressed. Also, upon further review and depending on the dataset(s) stored in your environment, your organization may be required to provide additional evidence in the form of artifacts related to subset of the DMP SAQ questions.

11. **Q: Can my organization have more than one DMP SAQ?**
    A: Yes, an organization can have multiple DMP SAQs. Each DMP SAQ evaluates a single computing environment used to store and process CMS data at an organization. Some organizations store and process CMS data within a single environment, whereas others might store and process CMS data in more than one environment. Even though multiple computing environments are allowed, organizations should make an effort to engage IT personnel and coordinate with others in the organization to avoid duplication or overlap.

12. **Q: Does my organization need to use its full legal name on the DMP SAQ?**
    A: Yes, CMS requires that the full legal name is used on the DMP SAQ. CMS also requires organizations to use their full legal name on all DUAs. The name on the DMP SAQ must match the name on the DUA (or the name of a collaborator) in order to be able to pair them. If the full legal name is not currently on the DUA, a request must be made through ResDAC to update the name on the DUA.

Approval of the DMP SAQ

13. **Q: What happens after we submit the DMP SAQ?**
    A: After your DMP SAQ is submitted, it will be reviewed by the DPSP. The DMP SAQ should be submitted as a Word document so that the DPSP can provide feedback. If there are any additional questions, DPSP will notify the point-of-contact. Once the DMP SAQ is successfully completed, DPSP will notify the organization if it has been approved.

14. **Q: Does my organization's DMP SAQ impact active DUAs?**
    A: As you work on completing your DMP SAQ, the DPSP team will request that you provide a list of all the active DUAs you would like applied to your DMP SAQ. Once your organization's DMP SAQ is approved, the DPSP team will coordinate with CMS to ensure that your active DUAs are paired to the appropriate DMP SAQ. If your organization has any DUAs that are NOT paired with an approved DMP SAQ, then CMS will not extend the DUA and may prohibit the organization from opening or extending any DUAs until the offending DUA is paired or closed. Please note, although the DMP SAQ pairing is necessary for extending a DUA, the extension is processed separately through CMS.

15. **Q: How long will DPSP take to review our organization's DMP SAQ?**
    A: Once the DPSP receives a DMP SAQ for review, the DPSP will acknowledge receipt within 24 hours. Your organization will be notified within 5-7 business days of the status of your DMP SAQ. Please note that the review times may vary and can depend on your organization's responses, evidence

needed, type of DUA request, and other factors. Please attempt to answer all questions as any blank responses can delay the review time.

16. **Q: After our organization's DMP SAQ has been approved can we make changes to our environment?**
    A: If you make changes to your organization's environment after your DMP SAQ has been approved, you will need to submit an updated DMP SAQ that highlights the changes that you made to the document. The updates will need to be reviewed and approved by CMS and the DPSP.

17. **Q: What if our organization has existing data that needs to be moved from one environment to the approved DMP SAQ environment?**
    A: Before moving any data the organization MUST submit a Data Transfer Plan along with the approved DMP SAQ summary report to CMS for review and approval. Contact CMS at DataUseAgreement@cms.hhs.gov for instructions on completing the Data Transfer Plan.

Additional Resources

The following additional resources can be found at https://resdac.org/request-form/dmp-saq:

- Data Management Plan Self-Attestation Questionnaire (DMP SAQ)
- Requirements & Guidance for Security & Privacy Controls
- Instructional Resources
    1. How to Establish a DMP SAQ
    2. How to Prepare for a DMP SAQ
    3. The DMP SAQ Process - Start to Finish
    4. How to Renew a DMP SAQ
    5. Crosswalking the DMP vs New DMP SAQ
    6. How to Update the DMP SAQ
    7. How to Identify the Data Custodian for the DMP SAQ