How to Prepare for a DMP SAQ

For new or existing DUA organizations required to complete the CMS Data Management Plan Self-Attestation Questionnaire (DMP SAQ)

Step 1: Understand the Terms and Provisions of the DUA

The CMS Data Use Agreement (DUA) for Research Identifiable Files (RIF) outlines data security baselines required for protecting CMS data. Review these provisions to understand the requirements for your organization to manage and store CMS data. The security and privacy provisions outlined in the DUA follow the CMS Acceptable Risk Safeguards (ARS) 3.1 data security framework. Review the DUA and the ARS publication to prepare for developing a Data Management Plan Self-Attestation Questionnaire (DMP SAQ).

Step 2: Identify and Understand the Computing Environment

You will need to identify and understand the information technology (IT) operations, software, hardware, and services that will be used to store and manage the CMS data. Your DMP SAQ will need to identify:

- the computing environment or server that will be used to manage and store the data; and
- the Data Custodian—the individual responsible for the observance, establishment, and maintenance of all the conditions of use to prevent unauthorized use for the environment identified in the DMP SAQ.

Step 3: Identify and Engage the Right Stakeholders and Policies

Once you have identified the computing environment that will store and process the CMS data, you will need to identify the key policies and stakeholders at your organization that will support your completion of the DMP SAQ. For example, the DMP SAQ requires the knowledge and identification of your organization's policies and activities for access controls to the computing environment utilized to store and process the CMS data. You will need to identify and engage a stakeholder(s) with a skillset and knowledge of security and privacy policies for the computing environment. As another example, the DMP SAQ requires an understanding of breach response policies and activities. You will need to identify your organization's breach response policy and the individuals involved in reporting operations. You should review the CMS ARS 3.1 publication for a full understanding of the security control families as part of your preparations for completing the DMP SAQ.

Step 4: Complete the DMP SAQ

Once you have completed the steps above, you are ready to complete your DMP SAQ. As you complete the DMP SAQ, be sure that you have responded to each DMP SAQ question and provided a policy citation or validation where necessary.

Step 5: Submit the DMP SAQ to the CMS Data Privacy Safeguard Program

When your DMP SAQ is complete, submit the DMP SAQ and policies, if policies are not linked in the document, to the CMS Data Privacy Safeguard Program at DPSP@cms.hhs.gov.

For more details on completing and submitting the DMP SAQ, see "How to Establish a DMP SAQ".

This guide is provided in support of the Data Privacy Safeguard Program (DPSP) by MBL Technologies, the authorized contractor for the DPSP. For questions, please contact DPSP@cms.hhs.gov.