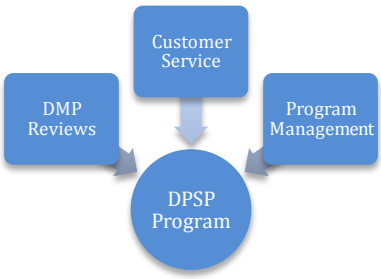
Data Privacy Safeguard Program

Office of Enterprise Data & Analytics

Division of Data and Information Dissemination

Overview

The Program



The Data Privacy Safeguards Program (DPSP) ensures the protection of CMS data that is disclosed to researchers- research identifiable files (RIF) which are disclosed for relevant research studies. **The primary objectives of the DPSP is to review requestor's Data Management Plan (DMP) submissions and provide guidance to researchers on how to implement effective, reasonable, and appropriate measures that protect CMS RIFs.** The DPSP consists of:

Data Management Plan Reviews

A Data Management Plan is a key document of each DUA request packet. In the DMP researchers are asked to explain the privacy safeguards they have in place for their particular research requests. The privacy safeguards that researchers are asked to respond on include administrative, physical, and technical safeguards, and incident response preparedness. These safeguards also correlate with specific sections of the researcher's data use agreement that gets signed by the researcher once their request for data is approved. Each DMP submission is evaluated to determine whether the researcher has explained its privacy safeguards in accordance with CMS information security and DMP guidelines. Researchers are explicitly asked, and are expected to reference written policies and procedures.

As part of a complete DMP review, the DPSP delivers:

(1) DMP Cover. The DMP Cover is the file that indicates the evaluation rating of the DMP. The ratings are:

- Green seal= approved for Privacy Board review
- Yellow seal= flagged for needed updates. Requestor is asked to review DPSP comments, make updates, and resubmit DMP for review.
- Red seal= DMP includes data safeguard concerns that need the attention of the Privacy Board (ex: foreign researcher, unsecure data transport practices, etc)

(2) DMP Review Checklist. The DMP Review Checklist is a question-by-question review of the Data Management Plan. As necessary, the DMP Review Checklist identifies any non-compliant security practices, provides recommendations for updates to practices and policies and makes note of any discrepancies in data security plans.

Customer Service

DPSP provides customer service to data requestors and the Research Data Assistance Center (ResDAC) for submitted DMPs. These activities include: reaching out to requestors to collect information needed to understand the data storage or sharing environment; collecting information related to collaborative projects and data transport across locations; supporting the completion of Collaborator Checklists; providing recommended updates to DMPs before final DMP review; and offering additional, as-needed support to requestors throughout the DMP review process. The contractor shall also provide ResDAC with DMP assistance in the form of regular updates for each DMP, plans for each DMP review schedule, delivery of a summary of evaluation and findings for each DMP, and other support to ResDAC staff.

Program Management

The DPSP provides the following program management functions to ensure that DPSP tasks are completed efficiently, effectively, and consistently and timely: Monthly status reporting, monthly invoicing, Weekly Status Report and meetings, weekly DMP queue, and ad hoc notification to CMS leadership of any data security issues.

MBL TECHNOLOGIES
data_privacy_safeguard_program@mbltechnologies.com
Monika Edwards, PM
monika.edwards@mbltechnologies.com