PMACS Data Use Agreement (DUA) Standard Operating Procedure

1. Purpose

The Privacy Act of 1974 requires the Centers for Medicare & Medicaid Services (CMS) to account for all disclosures of personally identifiable information (PII). CMS uses the DUA to account for all such disclosures. The CMS Privacy web site, http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html provides all the relevant information regarding CMS DUAs, the CMS Privacy Office and CMS' System of Records.

The "Privacy" web pages provide the processes for requesting CMS data that contains PII and that is protected by the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and which is releasable to:

1. Oversight Agencies
2. Federal Agencies (and their Contractors)
3. State Agencies
4. Researchers (Academic Institutions/Private Sector)
5. Providers

The Researcher Data Assistance Center (ResDAC) is a CMS contractor that provides free assistance to researchers interested in using Medicare and/or Medicaid data for their project/study. All requests from Researchers must be submitted via ResDAC for submission to CMS.

2. Scope

This procedure will be followed when requesting CMS data that contains PII and that is protected by the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

3. Responsibilities

The DUA applicant is responsible for completing and submitting the DUA application.
4. Procedure

DUA Applicant –
The DUA applicant is responsible for:

   a. General questions by the DUA applicant related to incident response and general security should be addressed by referring the applicant to:
      • The ISC Incident Response Policy - [http://www.upenn.edu/almanac/volumes/v53/n18/or.html](http://www.upenn.edu/almanac/volumes/v53/n18/or.html)
      • The ISC Computing Policy link - [http://www.upenn.edu/computing/policy/](http://www.upenn.edu/computing/policy/)
      • The PMACS Resource Environment document.

2. The applicant will discuss with his/her PI, how the data will be acquired from CMS. For example, will it be given to the PI on media, or transmitted electronically and if so, how will it be transmitted?

3. The applicant will determine who will need access to the information.

Note: DUA applicants who are not using PMACS services will be considered to be the DUA custodian.

DUA Custodian – Information Security Officer –
The PMACS Information Security Officer (ISO) is considered to be the custodian for PSOM related DUAs if the data will be centrally managed by PMACS, however Core Infrastructure (Pat) will be the operational custodian of the information.
The ISO will supply Core Infrastructure and Systems Administration with the following:

1. The CMS data, or information about how the data will be transmitted to PSOM.
2. List of users who need access to the CMS data.
3. Copy CSG in case system modifications need to take place.

IT Core Infrastructure and Systems Administration –
IT Core Infrastructure and Systems Administration will implement the CSM data repository, access solution, and user access privileges.

IT Core Infrastructure –
1. If applicable, maintain original CMS data, in safe.
2. Track usage.
3. Notify applicant if termination date has arrived without a DUA extension.

IT Systems Administration –
1. Creates the secure repository for the CMS data.
2. Sets up user access privileges.