Plan Overview

A Data Management Plan created using dmptool

Creator: Vanna Chi

Affiliation: Non Partner Institution

Funder: National Science Foundation (NSF)

Template: NSF-SBE: Social, Behavioral, Economic Sciences

Last modified: 11-26-2016

Copyright information:
The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customize it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal.
Roles and responsibilities

The Data Management Plan should outline the rights and obligations of all parties as to their roles and responsibilities in the management and retention of research data. It must also consider changes to roles and responsibilities that will occur should a principal investigator or co-PI leave the institution.

This data management plan will be delegated between each of the working participants of the data management team. The project will run from December 1, 2016 to June 30, 2017 (extended if need be). The project manager and supervisors are responsible for overseeing the project and ensure all working parties are conducting their roles in the project. The working participants are responsible for their specific duties (as specified in this plan). The supervisors who work under the data managers will be responsible for monitoring the project. A contract and weekly routine check-ups will be conducted to ensure all working parties are adhering to the rules and policies of the plan. If a role/responsibility needs to be transferred, the appropriate documents needs to be completed before any responsibilities are transferred to another individual. Only the data managers will have the responsibilities to make decision about the data once the original personnel are no longer available.

Expected data

The Data Management Plan should describe the types of data, samples, physical collections, software, curriculum materials, and other materials to be produced in the course of the project. It should then describe the expected types of data to be retained.

The data is the most important part of the project. The term data will be used loosely surrounding the project, used the context of specific data that was generated and collected from specific databases. I plan to collect raw data from ICPSR on the topic of Criminal Victimization and Perceptions of Community Safety in 12 United States Cities. This raw data will then be selectively imputed based upon the variables used and analyzed for the purpose of our project. The types of data that I plan on generating include various sizes that can be easily accessible. The files will be formatted in several different programs (standard formats): Open Document Format (ODF), ASCII, and comma separated values (csv). The data will be generated for the police department, outside agencies, and public citizens. The different types of data that will be created or included are various surveys discussing community perception of safety, and criminal victimization. The data will be created through previous reports and databases. We will utilize existing data by researching databases and archived files from past crime reports of victimization. All data will be preserved and statistical data will be shared with other agencies and the public.

Period of data retention

SBE is committed to timely and rapid data distribution. However, it recognizes that types of data can vary widely and that acceptable norms also vary by scientific discipline. It is strongly committed, however, to the underlying principle of timely access, and applicants should address how this will be met in their DMP statement.

The data obtained for the purpose of this project will be retained for 5 years. All data collectors, investigators, researchers, creators and supervisors will be able to access the data for the archived time period as long as they are in good standing with the project. The embargo period for political, commercial, patent, or publisher reasons will be after the 5 year data retention period. This is in place for the purpose of budget/costs and fees that occur to maintain and store
the data.

Data format and dissemination

The Data Management Plan should describe data formats, media, and dissemination approaches that will be used to make data and metadata available to others. Policies for public access and sharing should be described, including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements. Research centers and major partnerships with industry or other user communities must also address how data are to be shared and managed with partners, center members, and other major stakeholders.

The data obtained for the purpose of this project will be retained for 5 years. All data collectors, investigators, researchers, creators and supervisors will be able to access the data for the archived time period as long as they are in good standing with the project. The embargo period for political, commercial, patent, or publisher reasons will be after the 5 year data retention period. This is in place for the purpose of budget/costs and fees that occur to maintain and store the data.

Data format and dissemination

The files will be formatted in several different programs (standard formats): Open Document Format (ODF), ASCII, and comma separated values (csv). The reason for the standard formats is that it provides a great range for users to access the data. Due to the various types of formats, the data should be readily accessible by outside users. In order to gain access to the data, individuals are required to set up an account to the website. This allows users to gain many datasets published on the website, but also provides the creators information if any data is used for inappropriate means. The managing of sensitive information will be provided to users that have an affiliation with a college or university. There will not be any issues with privacy and ethics. This is due to the regulations that the project has set up to ensure compliance with the IRB protocol. Any information is obtained by collection of reports, research, and obtaining of additional information requires a release of information document and a signed document stating the understanding of the use of the data for purpose of research and collection of creation of future program to assist in crime prevention.

Data storage and preservation of access

The Data Management Plan should describe physical and cyber resources and facilities that will be used for the effective preservation and storage of research data. These can include third party facilities and repositories.

The long term strategy for storing, archiving, and preserving the data will kept on an electronic database for the purpose of storing and preserving data. After the 5 year retention period, I plan to divide the roles and responsibilities to all project staff. I plan to format the files for archiving in standard formats to be easily transferred to programs such as GIS. The procedures for backup and preservation of data include copying files onto a secure and safe drive that will be used for quick data restorations and emergency situations. All metadata included for the data will also be included in process of archiving, preserving, and data backup. This will allow for quick retrieval.

Additional possible data management requirements

More stringent data management requirements may be specified in particular NSF solicitations or result from local policies and best practices at the PI’s home institution. Additional requirements will be specified in the program solicitation and award conditions. Principal Investigators to be supported by such programs must discuss how they will meet these additional requirements in their Data Management Plans.

All participants planning to engage with operations of the project have to be subjected to a
criminal background check and fingerprint check. This is to ensure the safety of the data and other participants working on the project. All participants are required to submit a resume, complete an interview, and sign confidentiality waivers for information that is not to be presented to the public.