**Data Management and Security Template**

The PI must clearly describe how the data are to be managed, stored, and secured. The following questions serve as a template and should be presented and addressed within a stand-alone Data Management and Security document. The final document should be uploaded to section 44. **NOTE:** If you are using a third-party vendor to collect, manage, or store any of your data you may have to address specific institutional safeguards. Go to U-M Safecomputing to learn more about [Third-Party Security and Compliance.](https://safecomputing.umich.edu/protect-the-u/protect-your-unit/third-party-vendor-security-compliance) Depending on the nature of your data and third-party involvement, completion of specific forms may be required to document third-party security and confidentiality agreements.

1. **What is the nature of the data?**
	1. Electronic (text, audio, video, binary), hardcopy files, or biological specimens?
	2. Do the data contain protected health information, personal identifying information or other sensitive information?If yes, please precisely describe what these are.
	3. Are identifiers retained and linked to the data? Who will have access to the data? Who will have access to the identifiers?
	4. Are the data stripped of identifiers and the identifiers destroyed (anonymized data)? When will this take place?
	5. Are identifiers de-linked from the data and managed by use of a code? How are the identifiers, data files and key managed and secured? Who will have access to the identifiers, data files and key?

1. **Where and how will the data be stored and what security measures will be used for each?**
	1. Personal computer or laptop? University computer or laptop; location? Office file cabinet? Thumb/jump drive? Departmental or other U-M server; name and/or location?
	2. What security measures will be used with each (password protected; encryption; locked file cabinet in locked office, 128 bit encryption, etc.)?
	3. Who will have access to the computer/laptop/server/or files?
2. **How will data be transmitted or transported?**
	1. How will electronic files be transmitted? What measures are in place for secure transmission of data?
	2. How will hardcopy files be transported?
	3. How are the files and data protected while in transmission or when transported?
3. **When and how will data or records be deleted or destroyed?**
4. **Will cloud-computing resources be used?** (refer to UM policies at <http://www.safecomputing.umich.edu/cloud/> and at http://www.safecomputing.umich.edu/google/)
	1. What is the resource and what is the privacy policy for the resource?
5. **Will online data collection services be used?**
	1. What is the service/host? How is the survey accessed? How are data accessed by the study team? Will any non-secure services be used to access, collect, or transmit data (e.g., public portals, administrator logins, public WiFi networks, or public computers)?
	2. How are data moved/transmitted from the online host to the local storage device (computer, laptop, server, thumb drive, etc.)?
	3. Will the data be purged from the online host once downloaded to the local device? How and when?
	4. If the data are identifiable and sensitive, are confidentiality agreements in place with outside consultants or vendors?
6. **Will any datasets be used?**
	1. Is there a Memo of Understanding (MOU) or Data Use Agreement (DUA) associated with the use of these data?
	2. Does your security plan include all requirements contained in the MOU/DUA?