**Brief Protocol for Exempt Research Projects**

Use this brief protocol to provide an overview of your exempt research project. Use of this protocol is not necessary if you have already provided this information in the smartform application.

For projects collecting information that is **sensitive and identifiable under Exemption 2 or 3**, please complete the **Data Management and Security Questionnaire found on page 2 of this document.** The IRB must conduct a Limited Review to ensure that data are securely managed and stored before an exemption can be issued. As part of it’s Limited Review, the IRB must also review your **recruitment materials and consent materials**. Please upload these materials in response to item 5 (Exempt 2) or 8 (Exempt 3) in section 12 of the eResearch application. Again, this requirement to upload recruitment and consent materials *only applies to studies that collect sensitive identifiable information*.

1. Describe the subject population.
2. Explain how you will recruit subjects into the research (including when and where recruitment will be conducted and methods of recruitment (e.g. flyers, email, social media, face-to-face). It is not necessary to provide these materials.
3. Identify where the research will take place (i.e. the location of the research).
4. Briefly describe the research procedures that will be conducted with subjects, including a description of the data collection methods and any research interventions.

**Data Management and Security Questionnaire**

**Exempt 2 or 3 Projects Collecting Sensitive and Identifiable Data**

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?
2. **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?
3. **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?
4. **When and how will data or records be deleted or destroyed?**
5. **Will cloud-computing resources be used?** (refer to UM policies at <https://www.safecomputing.umich.edu/protect-the-u/protect-your-unit/safely-use-the-cloud/um-google> and at https://www.safecomputing.umich.edu/protect-the-u/protect-your-unit/safely-use-the-cloud)
   1. What is the resource and what is the privacy policy for the resource?
6. **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?