11. Confidentiality/Security/Privacy

11.1* Will the study team access any data that is linked to a subject's identity by name or other identifier or code? [Require Section 11-1]

- Yes
- No

11.2* Explain how the subjects' privacy will be protected.

11.3* How will the study team protect research records, data, and/or specimens against inappropriate use or disclosure, or malicious or accidental loss or destruction in order to protect the confidentiality of subject data?

Select all that apply:

- Locked office
- Locked cabinet or storage unit
- Restricted access
- Destruction of source data immediately after data collection (e.g., to preserve anonymity of a vulnerable population)
- Restrictions on copying study-related materials
- Access rights terminated when authorized users leave the project or unit
- Secure laptop
- Individual ID plus password protection
- Routine electronic back up
- Disaster recovery plan
- Encryption of digital data
- Network restrictions
- No non-UM devices are used to access project data, or any that are used to access project data use secure connections to communicate with U-M services (e.g. VPN – “virtual private network”)
- Security software (firewall, anti-virus, anti-intrusion) is installed and regularly updated on all servers, workstations, laptops, and other devices used in the project
- Safe disposition/destruction of data or devices, as appropriate (e.g., shredding paper documents, destroying disks or thumb drives, secure erasure of electronic media)
- Offsite storage
- Climate-control environment
- Other

If other please specify:

11.4* Will the research generate information that, if revealed, might place the subjects at risk of personal safety, criminal or civil liability, or damage to their financial standing, employability, or reputation [Require Section 11-2]

- Yes
- No

Examples of information, that if disclosed, might pose a risk to subjects include sexual matters, use of alcohol or drugs, stigmatizing or discriminating medical or mental health information. If you are applying for a...
11.5* Will data be provided to a repository as part of a data sharing agreement?
- Yes
- No
- Clear

A repository is a collection of data/specimens that are collected, stored and disseminated for research purposes. Researchers may be obligated by grant, contract or other agreement to submit data/specimens to a repository. For example, see National Human Genome Research Institute (NHGRI) or NIH Genome-Wide Association Studies (GWAS) Database of Genotype and Phenotype (dbGaP). Submission of data/specimens to certain repositories may require additional IRB certifications.

11.5.1* Please indicate the repository:
Select all that apply:
- GWAS/dbGap
- NHGRI
- ICPSR
- Other

If Other, please specify:

11.6* What will happen to the data and/or any specimens at the conclusion of this study?
Select all that apply:
- Destroy
- Retain for study recordkeeping purposes
- Retain for future research use - requires Section 11-4

11.6.1* If the data and/or specimens will be destroyed, describe the specific plan that will be employed following the required retention period.
THIS QUESTION IS REQUIRED IF YOU ANSWER 11.6 "Destroy."

11.6.2* If the data and/or specimens will be retained for study recordkeeping purposes, provide the following information (if covered in the attached protocol, please indicate section):
- expected duration of the retention period,
- any changes in the conditions or arrangements for storage of research data/specimens during the retention period, if different from those listed above in question 11.3.

THIS QUESTION IS REQUIRED IF YOU ANSWER 11.6 "Retain for study recordkeeping purposes"