

**Research Integrity Office**

Mail code **L106-RI**  
3181 S.W. Sam Jackson Park Road  
Portland, Oregon 97239-3098  
tel: 503 494-7887 | fax: 503 346-6808

*Protocol Checklist:*  
Confidentiality and Security

- 
- Describe how and where data/specimens will be stored and describe the final disposition of the data/specimens. Include:
- The location of data/specimens, who will have access to the data/specimens, and how access will be controlled.

**Example statements:**

Standard institutional practices will be followed as described in the OHSU Information Security and Research Data Resource Guide ([http://ozone.ohsu.edu/cc/sec/isg/res\\_sec.pdf](http://ozone.ohsu.edu/cc/sec/isg/res_sec.pdf)) to maintain the confidentiality and security of data collected in this study. Study staff will be trained with regard to these procedures.

Paper files will be stored in locked filing cabinets in restricted access offices at OHSU.

Electronic data is stored on restricted drives on the OHSU network.

Electronic data will be stored on encrypted computers.

Electronic data will be stored in a web-accessible REDCap database housed on an OHSU secure server.

Electronic data will be stored in a custom database housed on an OHSU secure server.

Access to data/specimens is restricted to study personnel.

Access to data requires OHSU ID/password authentication.

- Method of coding data/specimens, if applicable. Include a process to protect/maintain the key to the code and limit access to the key. Coding data does not make it anonymous or anonymized, unless you destroy the key.

**Example statements:**

Upon enrollment, subjects will be assigned a code that will be used instead of their name, medical record number or other personally identifying information. Electronic files for data analysis will contain only the subject code.

Codes will not contain any part of the 18 HIPAA identifiers (initials, DOB, MRN)

The key associating the codes and the subjects personally identifying information will be restricted to the PI and study staff. The key will be kept secure on a restricted OHSU network drive in a limited access folder.

- Plans for final disposition of the data/specimens, including release to a repository (either as part of this protocol or into another protocol) or plan to destroy at the end of study.
- Describe the process and requirements for requesting and releasing data/specimens.

**Example Statements:**

Data will be transferred to/from XXX in files using encryption. [Note: To encrypt an email, put 'secure:' in the subject line of the OHSU email.]

Data/specimens released to other investigators will be labeled with only the code.