Describe the nature of the data/specimens being collected:

- Protected health information (PHI, including dates), personal identifying information (PII) or other sensitive information.
- Electronic (text, audio, video), hardcopy files, or biological specimens?

Describe the type of technologies that will be used in the research study.

Example statements:

Data will be collected using (state all that applies): web-based site, survey, mobile app, wearable device, video conferencing, text messaging.

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 by the OHSU Information Security Directives at the following link: [http://www.ohsu.edu/xd/about/services/integrity/policies/ips-policies-info-sec-directiv.cfm#results](http://www.ohsu.edu/xd/about/services/integrity/policies/ips-policies-info-sec-directiv.cfm#results) to maintain the confidentiality and security of data collected in this study. Study staff will be trained with regard to these policies.

Paper files with restricted information in transit will be kept out of sight (such as in the vehicle trunk or under a seat.) Once the restricted information has arrived at the intended location (e.g. clinic, research site, or other site.), it will be secured (attended/secured/locked in a room or other container).

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

Electronic data will be stored on encrypted (state all that applies): computers, laptops, tablets, iPads, and/or smartphones.

Electronic data is stored (state all that apply):

- On restricted drives on the OHSU network.
- On a web-accessible REDCap database (housed on an OHSU secure server).
- On the cloud file storage solution provided by Box.com.
- In a custom database housed on an OHSU secure server (describe the database, software platform and security features of the platform).

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 a 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 email using encryption. [Note: For instructions, refer to the “Send a Secure or Encrypted OHSU Email” Help and How To article.]

Data files will be transmitted to/from XXX using a secure file transfer protocol (SFTP).

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

If you are proposing to use any system, technology or software application not provided by OHSU that processes, stores or receives data in this study, a **security review is required** (please refer to the OHSU Security Review Process).

In the event that a specific, limited deviation from the OHSU security policy is needed, you may request an exception for specific requirement(s). **Please refer to ISD-700-00016 - Information Security Policy Exceptions and Exceptions Form.**