*Please provide the following information regarding confidentiality of Protected Health Information (PHI).*

|  |  |
| --- | --- |
| **Protocol ID:**       | **Protocol Director:**       |

1. Specify [PHI](https://stanfordmedicine.box.com/shared/static/nodcdo1dq3y0gncfyv74kc3d78zi6ww6.pdf) (Protected Health Information) that may be used or disclosed in connection with this research study. PHI is health information linked to HIPAA identifiers. List BOTH health information AND HIPAA identifiers.

|  |
| --- |
|           |

1. You are required to comply with University Policy that states that ALL electronic devices: computers (laptops and desktops; OFFICE or HOME); smart phones; tablets; external hard disks, USB drives, etc. that may hold identifiable participant data will be password protected, backed up, and encrypted.

Stanford University IT approved platforms (<https://uit.stanford.edu/guide/riskclassifications>) should be used for data management. Consult with your Department IT representative for more information. Note any PHI data on paper must be secured in a locked environment.

For data security policies and links to encrypt your devices see <http://med.stanford.edu/irt/security/> and <http://www.stanford.edu/group/security/securecomputing/mobile_devices.html>.

[ ]  Please check here to affirm the above will be done.

1. Describe how data or specimens will be labeled (e.g. name, medical record number, study number, linked coding system) or de-identified. If you are de-identifying data or specimens, who will be responsible for the de-identification? If x-rays or other digital images are used, explain how and by whom the images will be de-identified.

|  |
| --- |
|            |

1. Indicate who will have access to the data or specimens (e.g., research team, sponsors, consultants) and describe levels of access control (e.g., restricted access for certain persons or groups, access to linked data or specimens).

|  |
| --- |
|           |

1. If data or specimens will be coded, describe the method in which they will be coded so that study participants' identities cannot be readily ascertained from the code.

|  |
| --- |
|            |

1. If data or specimens will be coded, indicate who will maintain the key to the code and describe how it will be protected against unauthorized access.

|  |
| --- |
|            |

1. If sharing data with others, describe how data will be transferred or transmitted (e.g., file transfer software, file sharing, email). If transmitted via electronic networks, confirm a Stanford University IT approved platform will be used (see <https://uit.stanford.edu/guide/riskclassifications>) or that data will be encrypted while in transit. Additionally, confirm appropriate agreements are in place to allow for the sharing (see <https://ico.stanford.edu/stanford-researchers/who-will-handle-my-agreement>).

|  |
| --- |
|       |

1. How will you educate research staff to ensure they take appropriate measures to protect the privacy of participants and the confidentiality of data or specimens collected (e.g. conscious of oral and written communications, conducting insurance billing, and maintaining paper and electronic data)?

|  |
| --- |
|           |