

Name of Principal Investigator



Project Title



Privacy and Data Security Plan for Principal Investigators

1) Non-sensitive Information/Data Use (including all de-identified data and de-identified patient information)

- Office number and location: _____
- Laboratory number and location: _____

2) Sensitive Information/Data Use (including all patient identifiable data, any animal studies whose focus is on pain and primate studies)

Please check one of the following boxes that apply to your study:

- This study **does not** collect or record sensitive data.
- This study **does** collect or record sensitive data.

****If this study does not collect sensitive data, skip to question 10.***

3) Hardcopy VA Sensitive Information/Data [VASI]

Will VASI in hardcopy form be stored for this study (includes paper, tape recording, film, etc.)?

- Yes No

- Office number and location: _____
- Laboratory number and location: _____

4) Electronic VASI

Is VASI stored on the VA secure network (do not include CPRS)?

- Yes No

If yes, identify the locations (server/folder etc).

Is VASI stored on a computer local hard drive (even temporarily) such as by specially obtained software?

- Yes No

If yes, identify the computer system and describe the sensitive data and how it is secured.



5) Images

Will images with personal identifiers (e.g. research [not clinical] records containing x-rays with patient names or record numbers) be used?

Yes No

If yes, indicate where images with identifiers are stored

- In the medical record (e.g., VistA imaging)
- With the study secured hardcopy information
- With the study electronic sensitive information

6) Photos with Faces or Recordings

(Note: If patients are involved, a special consent form (VA form 10-3203) will be required.)

Will photos with faces or recordings are stored?

Yes No

If yes, indicate where photos or recordings are stored

- With the study secured hardcopy information
- With the study electronic sensitive information

7) Identified Biological Specimens

Will biological specimens with subject identifiers (not code numbers) be stored?

Yes No

If yes, indicate where they are stored and the security measures employed.

8) Transporting and Sharing VASI

Is VASI collected outside of the VA? *(Note: An approved Authorization to Transport will be required.)*

Yes No

If yes, describe what is collected outside the VA and how it is secured in transit back to the VA

Is VASI transported outside of the VA for any purpose other than sharing (covered below)? *(Note: An approved Authorization to Transport will be required.)*

Yes No

If yes, describe what is transported outside the VA, for what purpose, and how it is secured in transit

Can VASI be disclosed to monitoring/auditing agencies by HIPAA Authorization? *(Note: The Research Office must be notified when monitors come to audit)*

Yes No

If yes, indicate the monitors/auditors that will have access by HIPAA Authorization



Will a copy of VASI be shared outside the VA for other purposes (e.g. collaborators or sponsors) by HIPAA Authorization?

Yes No

If yes, describe what is shared, who receives a copy of VASI, and how it is secured in transit

9) Any Other Relevant Details

Add any other privacy or information security details here

10) VA Data Security Rules and Responsibilities

By signing this form, I understand the following VA data security rules and responsibilities and that any deviation from the above data security plan will be first reported to my local ISO.

- All VA sensitive research information will be used and stored within the VA.
- All copies of VA sensitive research information will be used and remain within the VA.
- A property pass for equipment (i.e. Laptops etc...) must be obtained.
- Laptops or other portable media must be encrypted and password protected. NOTE: Contact the VA ISO for encryption issues.
- Data will not be transmitted as an attachment to unprotected e-mail messages. Data sent via mail or delivery service must be encrypted.
- Names, addresses, and social security numbers (real and scrambled) must be replaced with a code. NOTE: Names, addresses, and social security numbers (real or scrambled) may only be maintained on a VA server and documentation of the procedure by which the data were coded must remain in the VA.
- In the event of theft or loss of sensitive data or media containing VA sensitive data, I will report to the VA Police, Information Security Officer, and Privacy Officer immediately. Procedures for reporting theft or loss of sensitive data or the media such as a laptop, containing sensitive data are in place and familiar to the researcher and all other who have access to the data.
- Upon exit of any research team members (WOC, IPA, or VA paid), access to all sensitive data for this study will be terminated.
- Permission to remove VA sensitive data must be obtained from 1) immediate supervisor, 2) your ACOS/R&D, 3) the VA information Security Officer (ISO), and 4) the VA Privacy Officer. **If VA sensitive data is to be removed for this study; signatures from your supervisor, ACOS/R, Privacy Officer and ISO are needed in addition to your signature below:**

Name of Investigator (print)

Investigator Signature

Date



VA | Ralph H. Johnson
VA Medical Center

Signatures below needed for approval to remove sensitive information from VA:

| Name of Supervisor | Supervisor Signature | Date |
|---|----------------------|------|
| Amanda LaRue, Ph.D. ACOS for Research | Signature | Date |
| Laura Crawford or Chad Peek Privacy Officers | Signature | Date |
| Rito Anthony Brisbane Information Security Officer | Signature | Date |