****

Department of Veterans Affairs

Checklist for Reviewing

 Information Security in Research

**Resource Contacts**

|  |  |  |
| --- | --- | --- |
| **Information System Security Officer (ISSO) Name****Eduardo A. Lorenzo****Nichelle R. Downing****Prince M. Rogers** | **VA E-Mail Address****vhaechiso@va.gov** | **Phone Number** |
| **Research Compliance Officer (RCO) Name****Chelle X. Yin** | **VA E-Mail Address****Chelle.Yin@va.gov** | **Phone Number****720-857-5084** |
| **Records Management Officer (RMO) Name****Thomas M. Stear** | **VA E-Mail Address****Thomas.Stear@va.gov** | **Phone Number****720-723-6583** |

**Study Information**

|  |  |  |
| --- | --- | --- |
| Principal Investigator (PI) Name | VA E-Mail Address  | Phone Number |
| Study Title | Protocol Number (if available) |
| Study Contact Name      | VA E-Mail Address      | Phone Number      |
| Check all of the following that apply to this submission: |
| **Purpose of Submission**:[ ]  New Protocol [ ]  Continuing Review [ ]  Amendment [ ]  Only change is adding study personnel. If so, answer question 1 and proceed to PI Signature Section [ ]  Only change is study personnel have been removed from the study. If so, answer question 16 and proceed to Signature Section[ ]  Change in data collection/use/storage/transmission/disposition [ ]  Change in HIPAA Authorization [ ]  Change in VA Informed Consent [ ]  Change in Data Use Agreement **Enrollment Status:** [ ]  Open [ ]  Closed **Funding Source:**  [ ]  None [ ]  VA/Coop Study [ ]  NIH or Other Government Agency [ ]  Private Funding. Specify: **Data Use Information:**[ ]  Written Agreements Regarding Data Use [ ]  Data Use Agreement exists [ ]  Videos, pictures or audio recordings will be obtained [ ]  Study will require a contractor who will have access to VA sensitive data. Specify contractor and services:        |

|  |
| --- |
| **Check any of the following HIPAA identifiers that may be collected and recorded during the course of the study:** |
| **[ ]  Names** | **[ ]  Social security numbers or scrambled SSNs** | **[ ]  Device identifiers and serial numbers** |
| **[ ]  E-mail addresses** | **[ ]  Medical record numbers** | **[ ]  URLs (Universal Resource Locator)** |
| **[ ]  All elements of dates (except year) associated with an individual & any age over 89. Specify:**  | **[ ]  Health plan beneficiary numbers** | **[ ]  IP addresses (Internet Protocol)** |
| **[ ]  Telephone numbers** | **[ ]  Account numbers** | **[ ]  Biometric identifiers including finger and voice print** |
| **[ ]  Fax numbers** | **[ ]  Certificate or license numbers** | **[ ]  Full face photographic images and any comparable images** |
| **[ ]  All geographic subdivisions smaller than state. Specify:**  | **[ ]  Vehicle IDs and serial numbers including license plate numbers** | **[ ] Other unique identifying number, characteristic or code Specify:**  |
|  |

\*COORDINATOR/ PI—PROCEED TO SIGNATURE PG. 5\*

**Information Security Requirements**

|  |  |
| --- | --- |
|  | **These Columns To Be Completed by ISSO** **Based on a Review of Source Documents** |
|  | Requirement | Met  | Not Met | N/A | Comments |
| **1** | **Information Security Training: All study staff are up-to-date with VA Privacy and Information Security Awareness and Rules of Behavior training.** **(Ref: VA Directive 6500, ¶2a(5) and ¶3f(2) and VA Handbook 6500, Appendix D, ¶AT-2)** **[ ]  Yes [ ]  No**  |  |  |  |  |
| **2** | **Software: The study identifies specially obtained software that will be used, the source of the software, whether a license will be required, who will fund the license as well as any data that will be stored in temporary files on the computer’s hard drive.** **(Ref: VA Handbook 6500, Appendix D, ¶¶SA-6 and SA-7)** |  |  |  |  |
| **3** | **Web Applications: The study identifies any web application, as well as its security features, that will be used for such purposes as recruiting subjects, completing questionnaires or processing data.** **(Ref: VA Directive and Handbook 6102 and VA Directive and Handbook 6502.3)**  |  |  |  |  |
| **4** | **Data Flow: The study includes a description of the data collection, data flow and/or data management process that will be used during the course of the study.** **(Ref: VHA Handbook 1200.05, ¶10j)** |  |  |  |  |
| **5** | **Data Security Plan: Study describes how electronic data as well as paper records will be secured. (Ref: VHA Handbook 1200.05, ¶10j)** |  |  |  |  |
| **6** | **Data on a Hard Drive: The study identifies whether VA research data will be stored on the hard drive of a PC. If so, it is considered VA best practice to encrypt the PC. (Ref: VHA Handbook 1200.05, ¶10j)** |  |  |  |  |
| **7** | **Mobile Devices: The study states that all mobile devices will be encrypted and that the encryption is FIPS 140-2 validated. Note: All mobile/portable devices and media and any information transmitted to and from a wireless device must be protected with VA approved encryption technology that is FIPS 140-2 validated. (Ref: VA Handbook 6500, Appendix D, ¶AC-19)** |  |  |  |  |
| **8** | **Storage Location: The study identifies precisely where data and specimens will be stored, i.e. physical site, network location/server name (e.g. vhacbarsch), type of mobile storage device, building and room, etc. (Ref: VHA Handbook 1200.05, ¶10j and VA Handbook 6500, Appendix D, ¶Ac-19)** |  |  |  |  |
| **9** | **Removal of VA Sensitive Information from the VA Protected Environment: The study states whether or not research data is intended to be removed from the VA protected environment.** **(Ref: VHA Handbook 1200.05, ¶10j and VA Handbook 6500, Appendix D, ¶AC-19)** |  |  |  |  |
| **10** | **Protection of Media Stored at Alternate Site: If the study team plans to store VA sensitive information outside the VA protected environment, the study indicates by what method it will be protected. (Ref: VHA Handbook 1200.05, ¶10j and VA Handbook 6500, Appendix D, ¶PE-17)** |  |  |  |  |
| **11** | **Data Transmission: The study states how sensitive electronic information will be securely transmitted. Note: VA sensitive data or information may only be transmitted using VA-approved solutions such as FIPS 140-2 validated encryption. (Ref: VA Handbook 6500, Appendix D, ¶MP-1)** |  |  |  |  |
| **12** | **Data Backup: The study indicates that mobile storage devices do not contain the only copy of research information. Original electronic VA research data stored on a mobile device or outside the VA protected environment will be backed up regularly and stored securely within VA’s protected environment. (Ref: VA Handbook, Appendix D, ¶AC-19)** |  |  |  |  |
| **13** | **Shipping Data: Study indicates whether sensitive research data that must be sent via common carrier will be encrypted with FIPS 140-2 validated encryption if it is electronic and will be sent via delivery service with a chain of custody.** **(Ref: VA Handbook 6500, Appendix D, ¶AC-19 and VA Directive 6609)**  |  |  |  |  |
| **14** | **Data Return: The study includes a statement regarding what VA information will be returned to the VA, how the information will be returned to the VA, or plans for its destruction. Note: VA research data and information must be retained in accordance with the applicable VA Records Control Schedule (RCS), which is a set of rules established by the Federal government that states when Federal agencies are allowed to dispose of records. Prior to destruction of research records, the PI should contact the Records Management Officer for current policy.** **(Ref: RCS 10-1, VHA Handbook 1200.12, ¶¶9-10)** |  |  |  |  |
| **15** | **Data Destruction: The study includes a description of the methods that will be used to destroy data at the end of its life cycle. Note: If the protocol states information will not be returned to the VA, the protocol must state how and when the information will be destroyed. See note above in Question 39. (Ref: VA Handbook 6500.1, VHA Handbook 1200.12, ¶¶9-10, and RCS 10-1)** |  |  |  |  |
| **16** | **Termination of Data Access: The study states that removal of access to research study data will be accomplished for study personnel when they are no longer part of the research team.** **(Ref: VA Handbook 6500, Appendix D, ¶AC-2)** |  |  |  |  |
| **17** | **Incident Reporting: In accordance with VA policy, procedures are in place for reporting incidents, i.e. theft or loss of data or storage media, unauthorized access of sensitive data or storage devices or non-compliance with security controls. (Ref: VHA Handbook 1200.05, ¶10j; VHA Handbook 1058.01, ¶11.a; VA Handbook 6500, Appendix D, ¶AC-19, ¶PL-4, ¶IR-1, ¶IR-6 and VHA Handbook 6500.2))** |  |  |  |  |

**Information System Security Officer’s Signature Section**

|  |
| --- |
| **I have reviewed this study for compliance with VA information security policy. NOTE: If the ISSO has not recommended changes, the ISSO may proceed directly to the final signature.** **[ ]  Recommend Changes Without Further Review [ ]  Recommend Changes With Second Review Requested****Summary/Initial Signature or E-signature of Information System Security Officer Date**  |
| **[ ]  Study Complies With Policy** **Final Signature or E-signature of Information System Security Officer Date**  |

**Customizable Section**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**Comments Section**

|  |
| --- |
| **Use this section for additional comments by the study team.** |

**Principal Investigator’s Signature Section**

|  |
| --- |
| **As the Principal Investigator on this study, I have read the above document and agree the information contained herein is correct.****Signature or E-signature of Principal Investigator Date**  |

***Note: This checklist should become part of the IRB protocol file in accordance with VHA Handbook 1200.05, paragraph 38.***