SOP Title	APPENDIX 7 CONDUCTING INITIAL REVIEW OF SUBMISSIONS TO HSPB	SOP No.	UWS-HP-603
		Version	02.
Effective Date		Page	1 of 4

WRAIR Human Subjects Protection Branch
Human Subjects Research Studies
Data Security Supplemental Information Form

The following information is required by the WRAIR Human Subjects Protection Branch in addition to the Protocol Submission Checklist, in order to obtain information about the data security measures in place for the collected research data. The form should be completed by the Principal Investigator/WRAIR POC in conjunction with the data manager and/or Information Manager/Information Technology POC.
If information requested in this form is described within the protocol, the corresponding protocol section/page number(s) where the information is located in the protocol may be entered instead.

WRAIR Protocol Number:
Project/Protocol Title:
Version/Date:

1. Is PII/PHI data being collected/maintained for this protocol?

   ☐ Yes

   ☐ No

2. Describe the types of devices on which the PII/PHI or study data are stored? (Computers, Servers, tablets, SAN)

3. Describe the Physical location where the data will be stored.

4. Who is responsible for maintaining the data?

   a. List the roles of all personnel who will be authorized access to the data (Users, Managers, System Administrators and DBA's etc.) and how many of each?

   b. Do you require your privileged users to have any additional training and/or certifications for maintaining the security of the data? If so, what?

5. Describe the type of Physical Controls in place to maintain the confidentiality, integrity and availability of the data. (CCTV, ID Badges, Cipher Locks, Security Guards, Safes, Key Cards, other)

6. Describe the type of Administrative Controls in place to maintain the confidentiality, integrity and availability of the data. (Backups secured off-site, encryption of backups, methods to ensure only authorized personnel access to PII, regular monitoring of user's security practices, periodic security audits, other)

7. Describe the type of Technical Controls in place to maintain the confidentiality, integrity and availability of the data (Biometrics, Encryption of Data at Rest, Firewall, VPN, CAC, Encryption of Data in Transit, IDS, PKI Certificates, User ID/Password, Least Privilege Access, other)

8. Is data maintained on stand-alone systems or networked systems? Describe your system configuration.

    a. What type and version of antivirus software is being used?

    b. Other than virus scans, is vulnerability scanning of the data systems being conducted? If so, how often?

    c. What type of vulnerability management plan is in place?

    d. Has your network obtained any type of 3rd party accreditation in the last 3 years? (RMF, SoC)

9. If using username/password, do they meet DoD standards?

    ☐ Yes

    ☐ No

    a. How many characters must the password have?

    b. How often must the password be changed?

10. Is data being stored in a database?

☐ Yes

☐ No

a. If yes, is the database server securely behind a firewall?

b. How often are data backups performed on the database tables?

11. Are backups of all data performed?

☐ Yes

☐ No

If 'Yes':

a. What type of backup tool is being used?

b. How often are backups performed?

c. Are backups being sent to another location?

d. How often are the backups tested?

12. Is data being shared with third parties?

☐ Yes

☐ No

If 'Yes':

a. Who is the data being shared with?

b. Is there a written agreement (SLA, DUA) in place that discusses how data security will be maintained by both parties?

c. When external parties provide data, is the data scanned before being introduced to the network/system? If so, what tool is being used?

13. If a data breach should occur, describe the reporting processes in place. How quickly must WRAIR be notified?

14. If WRAIR data is being maintained by a 3rd party, how are you maintaining oversight or verifying the confidentiality, integrity and availability of the data?

15. Are any cloud services being used?

☐ Yes

☐ No

If 'Yes', please provide a brief description of the cloud service:

a. Who is the cloud service provider?

b. Does the cloud service provider meet FedRAMP Plus Moderate baseline requirements?

16. Once the protocol has been completed, what is the plan to dispose of the data?