

DEFENSE HEALTH AGENCY (DHA)



SYSTEM SECURITY VERIFICATION (SSV)

Related Data Sharing Agreement Application (DSAA) Number: [Entered by DHA Privacy Office]

Project Name:

Government Sponsor Name:

Company/Organization:

Date Submitted:



October 2013

The System Security Verification (SSV) is to be used by any entity that will store, transmit, process, or otherwise maintain Military Health System (MHS) data owned and/or managed by ' HHQH+ HDOK AJHQ\ (' + A), hereinafter referred to as MHS data, on an information system that has not been granted a Department of Defense (DoD) Authorization To Operate (ATO) or an Interim Authorization to Operation (IATO). The questions in the SSV are designed to address the requirements of DoD 8580.02-R, "DoD Health Information Security Regulation," which implements the Health Insurance Portability and Accountability Act Security Rule and sets forth administrative, technical, and physical safeguards. Additionally, questions in this SSV address the safeguards outlined in DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems". The Instruction establishes the policy for managing the security of unclassified DoD information on non-DoD information systems. The completed SSV will be considered part of the Data Sharing Agreement Application (DSAA) approval process. Once the DSAA is approved, the SSV and the DSAA will be incorporated into an executed Data Sharing Agreement (DSA).

This SSV must be completed by a technical representative of the data sharing requestor with the appropriate knowledge and skill to fully and completely address the information safeguards outlined in this document. It is recommended you provide any additional pertinent information for each question to provide the most complete answer.

In order to determine the privacy and security posture of your organization in regards to the requested data for this project, all information provided in this SSV must be confirmed and conclusive in their nature and not speculative or tentative.

Will this project work ONLY be performed on an information system that has been granted a DoD ATO or IATO? Yes No

If 'Yes', an SSV is not required. The DHA sponsor will need to provide written confirmation to the DHA Privacy Office of the existence of an ATO or IATO for the information system.

1. GENERAL SYSTEM INFORMATION

- 1) Please identify and list all organizations, contracting companies and government entities that are involved in providing, handling, accessing, processing, analyzing, and storing of the requested MHS/DHA data and describe their roles.

Organization Name(s)	Role(s)

- 2) Please identify the physical Primary Work Location (PWL) for this project.

Primary Work Location (PWL)

3) Does this project (for which the SSV is being submitted) involve developing an information system owned by or operated on behalf of the Department of Defense?

Yes No

If yes, please provide current certification and accreditation status.

2. DATA FLOW

Please complete the chart below by providing a description of how the data will be obtained and used by your organization. Of primary importance is a clear description of data flow between all parties identified above in the General System Information. Ensure data flow and associated safeguards are described. Include information about types of computer equipment used for the project (i.e., server, laptop or workstation), and information systems used to access and process MHS data.

(In addition to this information, you may provide a data flow diagram showing the movement of data from project start to finish. Please redact any and all sensitive information from this diagram prior to submission).

<p>Please provide a step-by-step description of:</p> <ol style="list-style-type: none"> 1. Receipt of data from ' + \$ to your organization 2. Dissemination of data to any and all authorized users once it is received by your organization, including explanation of backup process and final reporting at the end of the project 3. Disposition of data once no longer needed for project 	<p>Safeguards <i>(Please provide all technical and non-technical safeguard information for each step of the data flow)</i></p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Steps</p>	

--	--	--

3. REMOTE ACCESS & ALTERNATE WORK LOCATION (AWL)

- 1) Will the users be allowed to work from an alternate work location (AWL) (e.g., residence, hotel, hotspot) outside of the primary work location (PWL) stated in Section 1, General System Information?
 Yes No (If answered No, skip to the next section, 4. DATA STORAGE)

- 2) Please check all forms of data storage available for taking the data to the AWL and the physical and technical safeguards (including encryption) in place to protect them.

Formats of Data <i>(Please check all that apply)</i>		Safeguards <i>(Please provide information for each type of storage mechanism)</i>
<input type="checkbox"/>	Data stored on laptop and other mobile computing devices	Do you have full disk encryption implemented on the hard drive of the devices? <input type="checkbox"/> Yes <input type="checkbox"/> No Other safeguards:
<input type="checkbox"/>	Data on removable media (e.g., CD/DVD, portable hard drives, USB drives, etc.)	Will you be encrypting the data stored on the removable media? <input type="checkbox"/> Yes <input type="checkbox"/> No Other safeguards:
<input type="checkbox"/>	Data in printed format	Will the MHS data in printed format be protected to prevent unauthorized access? <input type="checkbox"/> Yes <input type="checkbox"/> No Safeguards:

- 3) When working from the AWL, will the users have remote access to the MHS data stored at the PWL?
 Yes No

- 4) Which of the following remote access methods are available to access the MHS from the AWL?

NOTE: Please ensure that methods for remote access are included in the data flow section.

- | | |
|---|---|
| <input type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> Unencrypted network connection |
| <input type="checkbox"/> Secure Socket Layer (SSL)/HTTPS | <input type="checkbox"/> Web portal access via HTTP |
| <input type="checkbox"/> Secure File Transfer Protocol (sFTP) | <input type="checkbox"/> FTP |

Other:

- 5) While working from the AWL, will the users have the technical means to save the data on their mobile computing devices?
 Yes No

4. DATA STORAGE at PRIMARY WORK LOCATION (PWL)

Please check all forms of data storage that will be used in this project and the physical and technical safeguards (including encryption) in place to protect them.

Type of Data Storage <i>(Please check all that apply)</i>		Safeguards <i>(Please provide information for each type of storage mechanism)</i>
<input type="checkbox"/>	Data in electronic format: <input type="checkbox"/> Server <input type="checkbox"/> Workstation	Safeguards:
	<input type="checkbox"/> Mobile device	Do you have full disk encryption implemented on the hard drive of the devices? <input type="checkbox"/> Yes <input type="checkbox"/> No Other safeguards:
<input type="checkbox"/>	Data on removable media (e.g., CD/DVD, portable hard drives, USB drives, etc.)	Will you be encrypting the data stored on the removable media? <input type="checkbox"/> Yes <input type="checkbox"/> No Other safeguards:
<input type="checkbox"/>	Data in printed format	Will the MHS data in printed format be protected to prevent the unauthorized access? <input type="checkbox"/> Yes <input type="checkbox"/> No Safeguards:

5. DATA BACKUP

Data Backup	
Is the data for this project backed up?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Where/by whom is the data backed up?	<input type="checkbox"/> In-House <input type="checkbox"/> Third-Party
Where is the backed up data stored?	<input type="checkbox"/> PWL <input type="checkbox"/> Off-Site (owned by your organization) <input type="checkbox"/> Off-Site (owned by third party) If stored off-site, describe method of transport to off-site location.
Please describe the safeguards in place to protect the backed up data.	

--	--

6. USER INFORMATION/DATA ACCESS

1) Please list all types of personnel who will be authorized to access MHS data (e.g., Users, Managers, System Administrators, Developers, etc.). Please indicate the purpose in which these personnel will serve in achieving the project objective.

2) Please check all statements that apply to your organization:

- Authorized users with access to MHS data have a unique user account and password.
- Level of access for each user is reviewed and granted in accordance with the required level of access needed to accomplish the project objectives.
- Our organization applies a "need-to-know" justification process in determining the level of access required for each employee and/or third party.
- Our organization has implemented policies and practices that require contractual arrangements to be made with teaming partners (organizations listed in Section 1 of this document) to ensure equal or better data protection on all shared MHS data (inclusive of third-party vendors).
- Our organization has implemented policies and procedures to ensure that MHS data is not accessed by unauthorized users.

7. COMPUTER/NETWORK TECHNICAL CONTROLS

1) The following protection devices are installed on the network (Please check all that apply):

- Network Firewalls
- Host based Firewalls on all workstations and servers
- Network Intrusion Prevention/Detection System
- System does not reside on a network

2) With regard to the system update and patching activities, please check all statements that apply to your organization:

- Computer Operating Systems (OS) are current with the latest patches and security updates in accordance with the organization's patch management policy.
- Anti-Virus software is deployed throughout the network on workstations and servers and is periodically updated.
- Anti-Spyware software is deployed throughout the network on workstations and servers and is periodically updated.

3) Which of the following safeguards are implemented on workstations in the case of inactivity?

- Automatic account log-off feature will log off the user after the predetermined time of inactivity, requiring the user to re-authenticate.
- Automatic screen lock will be activated after the predetermined time of inactivity, requiring the user to re-authenticate.

8. FAX AND VOICE TRANSMISSION

1) Are users are authorized to fax MHS data for this project? If so, please describe the formalized procedures and safeguards they are trained to follow.

2) Are users are authorized to utilize voice mail for communications containing MHS data for this project? If so please describe the formalized procedures and safeguards they are trained to follow.

9. PHYSICAL PROTECTION

1) With regard to physical security controls, please check the **one** statement that applies to your organization:

- All computing resources for the project (e.g., servers, workstations, laptops) are behind locked office doors and there are other safeguards preventing unauthorized physical access to the systems.
- Some computing resources are behind locked office doors and some workstations are not protected by locked doors (e.g. Computers placed in cubicles).
- None of the computing resources are protected by locked office doors.

2) Please check all access controls that apply to your organization's physical protection. Please identify other access controls that apply to your organization:

- Security guards
- Cipher locks
- ID Badge
- Other:

10. MEDIA PROTECTION (Electronic and Hard Copy)

1) Briefly describe the procedures you will use for removing MHS data from the information system resources when no longer needed for this project. Ensure that this information coincides with the information in your DSAA, Certificate of Data Disposition section.

2) With regard to reusable media protection, please check all policies and procedures implemented in your organization:

- Policy/procedure on sanitizing or destroying data from disks, hard drives, and/or CDs.
- Policy/procedure on proper disposal of printed (hard copy) data (i.e., shred or burn).

3) With regard to hardware inventory tracking, please check all policies and procedures that are implemented in your organization:

- Records are created and maintained to track each instance of computer equipment issuance to individual employees and/or internal organizations.
- Records are updated when custodianship of a hardware is changed from one employee or team to another.
- Records are updated and equipment is retrieved from each individual leaving the organization.

11. AUDIT

1) Are security audit controls implemented that record and examine user activity on the information system where the MHS data is processed and stored?

- Yes No

2) Please specify the information system components where auditing is implemented (e.g., server, workstation, laptop)

3) For each component, please list what events and/or activities are logged and reviewed.

4) Please indicate the frequency of the review required by your policies.

12. INCIDENT RESPONSE

1) With regard to your organization's Incident Response program, please check all that apply:

- There is a formalized organization-wide Incident Response program in place.
- The organization's Incident Response program includes detailed response procedures for privacy breaches and security incidents involving MHS data.
- Employees are trained regarding their responsibilities to report incidents and have an understanding of what constitutes a privacy breach and security incident.

2) If any, please state the circumstances of network or system breaches in your organization and the courses of actions taken to restore and ensure system integrity.

13. TRAINING AND AWARENESS

With regard to employee training and awareness, please check all that apply to your organization.

- Employees are required to receive initial and follow up refresher training periodically.
- Training includes topics relating to privacy and security.

14. ADDITIONAL COMMENTS:

The following signatories acknowledge that the information provided in this SSV is truthful and accurate, and that all necessary security measures will be taken to secure any and all DoD controlled unclassified information (CUI). In addition, the signatories acknowledge that any violation of satisfactory assurances provided herein will constitute non-compliance with DoD Health Information Security Regulation (DoD 8580.02-R, C 2.10.1.2). If your DSAA is approved, authorizing you to obtain MHS data owned or managed by '+\$', such approval is contingent upon the system descriptions and safeguards provided herein. By signing below, the Data Sharing Requestor understands that he/she is required to promptly notify the DHA Privacy Office of any change to information systems and safeguards, and further understands that this SSV is binding upon and will inure to the benefit of the Data Sharing Requestor and his/her respective successors and/or assignees.

Person Completing this System Security Verification:

(Name and Rank/Title of Technical Representative - Typed or Printed)

(Company/Organization)

(Business Street Address)

(City/State/ZIP Code)

(Business Phone No. including Area Code/Business E-Mail Address)

(Signature)

(Date)

Data Sharing Requestor:

(Name and Rank/Title - Typed or Printed)

(Company/Organization)

(Business Street Address)

(City/State/ZIP Code)

(Business Phone No. including Area Code/Business E-Mail Address)

(Signature)

(Date)

Privacy Statement

System Security Verifications are project or contract-specific, not individual data user-specific. Only the names and professional contact information of the Data Sharing Requestor and Technical Representative should be listed. The names and contact information for the listed individuals are maintained so information and notices can be sent to these individuals. This information may be protected under the provisions of the Privacy Act of 1974 and only released as permitted by law.
