Health Insurance Portability and Accountability Act (HIPAA) Safeguard Review of Non-Federal Systems

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

Project Name:

Company/Organization:

Government Sponsor Name:

Date Submitted:

October 2020

This template is to be used by any entity that will store, transmit, process, or otherwise maintain Military Health System (MHS) personally identifiable information (PII) and/or protected health information (PHI), which are specific privacy categories of controlled unclassified information (CUI), owned and/or managed by the DHA, hereinafter referred to as DHA data, on an information system that has not been granted a Federal Government Authorization To Operate (ATO). This document is designed to address the privacy requirements of Department of Defense (DoD) Instruction (DoDI) 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," DoDI 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," and National Institute of Standards and Technology (NIST) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." The completed document is a part of the DSAA approval process.

This template 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 the above references.

In order to determine the privacy and HIPAA security posture of your organization in regard to the requested data for this project, all information provided must be up-to-date and current in its nature, not speculative or tentative. Upon completion of this review, the DHA may request inspection of supporting policies/procedures, information system(s) and, the facility where the work will be performed.

Will DHA data ONLY be used on an information system that has been granted a Federal ATO?

☐ **Yes** ☐ **No**

If 'Yes', is this a DoD ATO?

☐ **Yes** ☐ **No**

If 'Yes', this review is not required. The DHA sponsor will need to provide written confirmation to the DHA Privacy Office of the ATO for the information system that approves specific types of DHA data (e.g., PII/PHI/ Limited Data Set (LDS)).

If 'No', please provide written confirmation to the DHA Privacy Office of the other Agency's ATO for the information system that approves specific types of DHA data (e.g., PII/PHI/LDS).

---

1. GENERAL SYSTEM INFORMATION

a) 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 DHA data and describe their roles.

Organization Name(s)	Role(s)

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

PWL

c) Please identify the information system where the DHA data will be stored.

Information System

d) Will DHA data be retrieved from the information system by a unique identifier?

☐ Yes ☐ No

If yes, has a System of Records Notice (SORN) been identified for the system?

☐ Yes ☐ No

Which SORN?

If no, please describe the purposes for which will you be using the DHA data.

2. <u>NIST 800-171 REQUIREMENTS</u>

a) Have you completed a System Security Plan (SSP) based on the security requirements found in NIST 800-171 for the information system where the DHA data will be stored?

☐ Yes ☐ No

If yes, please include a copy of the SSP as an attachment. If No, please complete the one on the NIST 800-171 webpage.

b) Have you completed a Plan of Actions and Milestones (POA&M) for any unimplemented requirements in your SSP?

☐ Yes ☐ No

If yes, please include a copy of the POA&M as an attachment. If No, please complete the one on the NIST 800-171 webpage.

c) Does your contract include Defense Acquisition Regulations System (DFARS) Clause 252.204-7012 which states that any, and all, contractors to DoD who will handle CDI must complete an SSP and POA&M?

☐ Yes ☐ No

If no, do you agree to abide by those requirements? Failure to abide by the DoD requirements could result in a denial of your DSAA.

☐ Yes ☐ No

3. <u>DATA FLOW</u>: Provide a description of how the DHA data will be obtained and used by your organization. Of primary importance is a clear description of data flow between all parties and information systems used to access and process DHA 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).*

Data Flow

4. USER INFORMATION/DATA ACCESS: Please list **all** types of personnel who will be authorized to access or may encounter DHA data (Users, Managers, System Administrators, Developers, etc.). Please indicate the purpose in which these personnel will serve in achieving the project objective.

Roles of Users and Number of Each Type:

Types of Users/Number of Each Type	Users Purpose

5. CLOUD COMPUTING

a) Will the DHA data be stored in a commercial cloud service provider?

☐ Yes ☐ No

If yes, please answer the following:

b) Who is the commercial cloud service provider?

c) Have you ensured that the cloud service provider meets FedRAMP Plus Moderate baseline requirements, to include Impact Level 4: Controlled Unclassified Information?

☐ Yes ☐ No

6. ADDITIONAL HIPAA SPECIFIC QUESTIONS: If the DHA data you are requesting is determined to be PHI or LDS as defined by DoDM 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," please answer the following.

a) Do you have a contingency plan for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, or natural disaster) that damages systems that contain electronic PHI (ePHI)?

☐ Yes ☐ No

If yes, do you periodically test and revise the plan?

☐ Yes ☐ No

If no, how do you plan to respond in the event of an emergency?

b) Do you have a sanction policy that applies appropriate sanctions against workforce members who fail to comply with the HIPAA Privacy and Security requirements?

☐ Yes ☐ No

If yes, please provide the sanctions for a failure to follow appropriate standards for safeguarding ePHI.

If no, how do you respond to those who fail to safeguard ePHI?

c) Do you have safeguards in place to protect the ePHI from improper alteration or destruction?

☐ Yes ☐ No

If yes, please describe those safeguards.

If no, how will you safeguard the ePHI from improper alteration or destruction?

d) Do have procedures in place to verify that the ePHI has not been altered or destroyed in an unauthorized manner?

☐ Yes ☐ No

If yes, please describe those procedures.

If no, how will you ensure that the ePHI has not been altered or destroyed in an unauthorized manner?

7. <u>ADDITIONAL COMMENTS</u>:

The following signatories acknowledge that the information provided in this document is truthful and accurate, and that all necessary security measures will be taken to secure any and all DHA data. In addition, the signatories acknowledge that any violation of satisfactory assurances provided herein will constitute non-compliance with DoDI 8580.02, Enclosure 4.i. If your DSAA is approved, authorizing you to obtain DHA data owned or managed by DHA, 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 document 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 Form:

(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

A HIPAA Safeguard Review of Non-Federal Systems is 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.