Internal Use Only

DSAA #

TRICARE Management Activity
Data Sharing Agreement Application

The Data Sharing Agreement Application (DSAA) is designed to assist the TRICARE Management Activity (TMA) Privacy and Civil Liberties Office (Privacy Office) with its consideration of requests involving TMA managed data. Each data request is reviewed for compliance with regulatory requirements.

The Privacy Office determines whether the requested data use complies with applicable privacy and security requirements and neither grants system access nor provides data extractions. To obtain the requested data, however, the system program office responsible for granting system access, or the office responsible for providing any data extraction, may require prior Privacy Office approval.

This application to request data must be completed by both the Applicant and the Government Sponsor, defined below. As the DSAA is project or contract-specific, not individual data user-specific, only the names of the Applicant and Government Sponsor should be specifically listed. Upon approval, this application will be incorporated into a Data Sharing Agreement (DSA). See Appendices A - D for applicable requirements, responsibilities, definitions, acronyms, and examples.

1. PROJECT TITLE

2. CONTACT INFORMATION

a. **Applicant:** The individual with oversight of, and responsibility for the data use. If contractors will access the data, the Applicant must be an individual from the primary contracting organization who has data-use oversight. The Applicant is responsible for primary contractors and subcontractors, as applicable.

Applicant is (*check one*):

- ☐ Contractor
- ☐ Government Employee or Service member
- ☐ Researcher in DoD-Supported Study
- ☐ Academic Researcher
- ☐ Other (*describe below*):

Enter Applicant's Contact Information:

Applicant Name

Title/Rank

Company or Organization

Street Address

City

State

Zip

Country

Phone Number

E-mail Address

Internal Use Only
DSAA #

CONTACT INFORMATION (CONTINUED)

b. **Government Sponsor:** The individual that is ultimately responsible for the requested data use.

Enter Government Sponsor's Contact Information:

Government Sponsor's Name

Title/Rank

Office or Agency

Street Address

City

State

Zip

Country

Phone Number

E-mail Address

3. FUNDING ARRANGEMENT INFORMATION

a. What type of arrangement was executed to fund the project related to this requested data use?

1. Select the appropriate choice:
   - ☐ Contract: #
   - ☐ Grant: #
   - ☐ Cooperative Research and Development Agreement (CRADA): #
   - ☐ Other type of funding arrangement: #
     Describe:
   - ☐ Not Applicable *(Explain i.e., government only)*:
2. Option Year Period of Performance Dates:
   Not funded by contract? List expected start and completion dates

b. Other Primary Contracting Organizations

Each primary contracting organization using the data is required to submit a separate DSAA

Will other primary contracting organizations be included in this data use? If so, list each below.

c. Subcontractor Organizations

List each subcontracting organization that will have access to or use of the requested data

1. Subcontracting organization(s):

2. Briefly describe how subcontractor(s) will use the requested data:

Internal Use Only
DSAA #

FUNDING ARRANGEMENT INFORMATION (CONTINUED)

a. Business Associate Agreement (BAA)

1. Has BAA language been incorporated into the above-referenced contract, grant, CRADA, or other project documentation?

☐ Yes ☐ No

2. If this response is "No," please explain why the BAA is not applicable to your data use:

If the Privacy Office determines that this application involves the access to or use of data elements containing protected health information (PHI), a modification to incorporate BAA language into the funding arrangement (or other project documentation) may be required before the DSAA is approved.

*BAA language may be found **on the Privacy Office website**.*

4. PROJECT DESCRIPTION / JUSTIFICATION FOR DATA USE

Describe the project referenced in section 3, including a justification of why the requested data are needed.
If this response exceeds the space available, attach additional pages

Internal Use Only
DSAA #

5. DATA DE-IDENTIFICATION, PUBLISHING AND REPORTING

a. Will individually identifiable data be de-identified in compliance with DoD 6025.18-R? If so, complete the section below. *See Appendix B for requirements*

1. Indicate the method to be used for de-identification: ☐ Expert Determination
   ☐ Safe Harbor

2. Describe the steps intended for the data de-identification:

3. Who will de-identify the data?

4. List individual's qualifications for de-identifying data (i.e., statistician, etc.):

5. Will identifiers associated with all 18 data categories be removed?
   ☐ Yes ☐ No

6. If identifiers will remain, list those identifiers below (e.g., dates or addresses):

7. Is any information related to this data request intended to be published, reported, or otherwise released?
   ☐ Yes ☐ No

b. If the question 7 is marked as "Yes," address the two items below. If marked as "No," skip to section 5

1. Indicate the type of information that will be published, reported, or otherwise released:

2. Describe the method intended to ensure minimal risk of identifying / re-identifying individuals:

Internal Use Only
DSAA #

6. DATA FLOW, USE AND MANAGEMENT

a. Describe the intended flow, use, and storage of the requested data from time of receipt through the project's duration. Include diagrams and or illustrations as separate attachments, if necessary. *See Appendix D*

b. Check any item(s) below that apply to the requested data use (if submitting SSV, skip to section 7):

1. ☐ Data are accessed while teleworking
2. ☐ Data are received on removable media
3. ☐ Data at rest are encrypted
4. ☐ PII / PHI are accessed remotely
5. ☐ Data are backed-up on removable media
6. ☐ Data are received by email
7. ☐ Data in transit are encrypted
8. ☐ PHI / PII are transported or stored offsite
9. ☐ Data are accessed by login using the following system access level:

10. ☐ Data are received as an extraction, provided by:

11. Equipment intended for data use is: ☐ Government Furnished Equipment (GFE)
    ☐ Non-government Furnished Equipment

12. How often will the data be accessed?

Internal Use Only
DSAA #

7. FOR RESEARCH REQUESTS ONLY

a. Complete this section if data will be used for a systematic investigation, intended for generalizable knowledge, involving information about individuals. Otherwise, skip to section 8.

- The protocol must be approved by an Institutional Review Board (IRB)
- The TMA Human Research Protections Office (HRPO) must review the research documentation
- The Sponsor must ensure that any publication/release complies with DoD requirements
- For more information, visit the TMA Human Research Protection Program web page

1. Title of Research Project Protocol:

2. Principal Investigator's Name:

3. Principal Investigator's E-Mail Address:

4. Principal Investigator's Telephone Number:

5. Principal Investigator's Mailing Address:

6. Has this project been approved by an IRB? ☐ Yes ☐ No

7. Has this research been submitted for TMA Human Research Protections Official Review?
(CDO is required for DSAA approval)
☐ Yes CDO: #
☐ No

8. Does this research involve a survey or information collection from ten (10) or more individuals?
☐ Yes ☐ No

9. If question 8 is "Yes," indicate type of approval: ☐ Report Control Symbol (RCS)
☐ Office of Management and Budget (OMB)

10. RCS / OMB Determination Number:

11. RCS / OMB Expiration Date:

b. Answer the question below if this request involves modifying or renewing the previously approved DSA for this protocol. If the protocol has changed, and if the request involves PHI, the TMA Privacy Board will be advised.

1. Has there been any change to this protocol since the previous DSA approval? ☐ Yes ☐ No

2. Describe protocol changes, if any:

Internal Use Only
DSAA #

8. SOURCE AND TYPE OF DATA

a. Indicate the TMA managed system(s) from which the requested data will be obtained:
- Requested data must be limited to the minimum necessary for accomplishing the described purpose.
- The type of agreement (PII excluding PHI, PHI, Limited Data Set or De-identified) is determined by the specific data elements requested, or by the type of data that may be accessed via direct login.

☐ AHLTA	☐ ESSENCE	☐ PDTS
☐ M2	☐ MDR	☐ PEPR
☐ TMDS	☐ CHCS	☐ Other (specify):
☐ DMHRSi	☐ Essentris	

b. Identify whether the requested data will include only a set of specific data elements, or if all the data elements from a system file are needed. Check any that apply and provide details as directed below.
Note: Requesting all data elements within a system will be examined for "minimum necessary" compliance

1. ☐ This request includes *specific* data elements from the following system(s):

2. ☐ This request includes all data in the following system(s)

→ Provide justification for requesting the use of *all* data within a system:

c. To specify files and data elements, choose the applicable Data Request Template (DRT) below:

Each DRT is available on the templates page of the Privacy Office website
- The "DRT Military Health System Data Repository (MDR) Extractions," reflects the most current MDR data dictionary (*Enable MACROS for this DRT to print out only the chosen data elements).*
- The "General Data Request Template" may be used to list data from systems other than MDR.
- The "DRT_Access by Login" may be used to list data intended to obtain via direct login.

d. The Privacy Office does not confirm data-use compliance for data obtained from non-TMA managed systems. Permissions to use non-TMA managed data should be obtained from the respective system managers.

1. Will the requested data be potentially merged, linked, or otherwise associated with data from any other sources outside of TMA?

☐ Yes ☐ No

2. If "Yes," explain why, and by what method the TMA and non-TMA data will be associated?

3. List the non-TMA managed systems:

Internal Use Only
DSAA #

9. ADDITIONAL INFORMATION

For further privacy assessment, please respond to each of the following questions:

1. Will PII be electronically collected, maintained, used, or disseminated?

☐ Yes ☐ No

2. If yes, provide the name of the database or system where PII are (or will be) stored:

3. Will an item, collection, or grouping of information be created with the intent of retrieving an individual's information using a unique identifier?

☐ Yes ☐ No

4. If yes, provide the System of Records Notice (SORN) number applicable to the system in which the data will be stored:

10. SYSTEM SECURITY INFORMATION

If data will be stored, processed, maintained or used on DoD approved equipment, include the DoD Authorization to Operate (ATO), Interim Authorization to Operate (IATO) or National Institute of Standards and Technology (NIST) Certification. Consult the technical representative responsible for maintaining the computing resources proposed for this data use if necessary (e.g., Information Assurance Officer).

Provide DoD Approval Information for each system on which TMA data will be used:

1. List Each System or Network	2. Indicate Type of Approval:	3. Expiration Date

4. List any organizations, indicated in sections 3b and 3c, that will store, process, maintain or use the requested data on equipment that is not DoD approved (e.g. contractor, academic institution equipment):

If the requested data contain individual identifiers, a System Security Verification (SSV) template must be completed by each organization indicated in section 10b.

The SSV is available on the DSA templates page of the Privacy Office web site.

11. APPLICABLE SUPPORTING DOCUMENTATION

Check all documents that will be submitted in support of this DSAA:

☐ Data Flow, Use and Management
☐ Data Request Template(s)
☐ SSV Template(s)
☐ Other (briefly describe):

Internal Use Only
DSAA #

12. CERTIFICATIONS

The electronic initials provided below, by the Applicant and Government Sponsor, verify that the information provided in this DSAA is truthful and accurate. The undersigned agree to notify the Privacy Office promptly if any project change(s) affect this DSAA.

The parties acknowledge that after the DSAA is approved, the Privacy Office will send the appropriate DSA to the Applicant (referenced as the Recipient on the DSA) and the Government Sponsor for signature. The Recipient/Sponsor signed DSA will then be returned to the Privacy Office for final Privacy Office signature. Upon Privacy Office signature, the DSA will be executed, incorporating the DSAA.

DSA Applicant Certification

Date:

By electronically initialing this application, I certify that this application is submitted with my consent.

Government Sponsor Certification

Date:

By electronically initialing this application, I certify that this application is submitted with my consent.

Privacy Office Internal Use Only
DSAA Approval

Data Sharing Compliance Manager
TRICARE Management Activity Privacy and Civil Liberties Office
7700 Arlington Boulevard, Suite 5101
Falls Church, VA 22042-5101
703-681-7500

Internal Use Only
DSAA #

TRICARE MANAGEMENT ACTIVITY
DATA SHARING AGREEMENT APPLICATION
APPENDIX A
RESPONSIBILITIES

APPLICANT/RECIPIENT RESPONSIBILITIES:

- Agree to and execute a DSA after the DSAA is reviewed by the Privacy Office Performing a sponsored project or study under a Government contract
- Ensure the project abides by the submitted protocol and the stipulations as stated in the DSA
- Request data and assume physical or contractual liability for preserving the data integrity
- Provide and maintain accurate and complete responses to the DSAA
- Notify the Privacy Office of any changes to the data use, storage or disclosure
- Ensure that Business Associate Agreement (BAA) requirements, if applicable, are fulfilled
- Confirm that TMA breach notification and response procedures are followed (in the event of potential or actual loss, theft, or compromise of data) as outlined on the Privacy Office website: **http://www.tricare.mil/tma/privacy/breach.aspx**
- Submit a completed Certification of Data Disposition (CDD) to the Privacy Office no later than 30 days after the expiration of the DSA

GOVERNMENT SPONSOR RESPONSIBILITIES:

- Agree to and execute a DSA once the DSAA is reviewed by the Privacy Office
- Provide Applicant/Recipient oversight for the duration of the DSA project
- Serve as the Government (military or HA/TMA civilian personnel) Point of Contact
- Affirm scientific merit, feasibility and usefulness in relation to the Military Health System (MHS) mission, goals, and objectives
- Examine the project to avoid both duplication and unnecessary generation of data
- Assure that the data outcomes benefit DoD
- Verify compliance with applicable standards for privacy and security of data
- Confirm that any publication or release of data, results, or findings adheres to DoD requirements
- Maintain current contact information with the Privacy Office
- Certify accurate and complete responses to the DSAA
- Ensure that the BAA requirements, if applicable, are fulfilled
- Notify the Privacy Office of any changes to the data use, storage or disclosure
- Endorse timely DSA renewal, if necessary
- Assure that TMA breach notification and response procedures are followed (in the event of potential or actual loss, theft, or compromise of data) as outlined on the Privacy Office website: **http://www.tricare.mil/tma/privacy/breach.aspx**
- Endorse the submission of a CDD no later than 30 days after the expiration of the DSA

TRICARE MANAGEMENT ACTIVITY
DATA SHARING AGREEMENT APPLICATION

APPENDIX B

DEFINITIONS AND ACRONYMS

DEFINITIONS

- Accreditation Decision: A formal statement by a Designated Accrediting Authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an Authorization to Operate (ATO), Interim Authorization to Operate (IATO), Interim Authorization to Test (IATT), or Denial of an Authorization to Operate (DATO).
- De-identified PHI: Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.
- Information system: For the purpose of this application, a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced information technology (IT)-based processes, and platform IT interconnections.
- Limited Data Set: A limited set of identifiable patient information as defined in the Privacy Regulations issued under the Health Insurance Portability and Accountability Act (HIPAA).
- Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, date and place of birth, mother's maiden name, biometric records, including any other personal information that is linked or linkable to a specified individual.
- Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by TMA in its role as an employer.

DE-IDENTIFICATION REQUIREMENTS

- The HIPAA Privacy Rule provides two methods by which health information may be de-identified. Satisfying either method would meet the standard in §164.514(a).

1. The Expert Determination Method:
    - A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
    - Documents the methods and results of the analysis that justify such determination;
2. The Safe Harbor Method: The identifiers of the individual or of relatives, employers, or household members of the individual, as defined by the Privacy Rule, are removed.

TRICARE MANAGEMENT ACTIVITY
DATA SHARING AGREEMENT APPLICATION

APPENDIX C

ACRONYMS AND REGULATORY REQUIREMENTS

ACRONYMS FOR TMA MANAGED SYSTEMS

CHCS	Composite Health Care System
DMHRSi	Defense Medical Human Resources System – internet
EAS	Expense Assignment System
PDTS	Pharmacy Data Transaction Service
M2	Management Analysis and Reporting Tool
PEPR	Patient Encounter Processing & Reporting
MDR	MHS Data Repository
TMDS	Theater Medical Data Store

FEDERAL LAW

Privacy Act of 1974, as amended (5 U.S.C. 552a)

Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (45 C.F.R. Parts 160 and 164)

DEPARTMENT OF DEFENSE (DOD) REGULATIONS

DoDD 5400.11, DoD Privacy Program, May 8, 2007

DoD 5400.11-R, DoD Privacy Program, May 14, 2007

DoDI 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs, December 2, 2009

DoD 6025.18-R, DoD Health Information Privacy Regulation, January 24, 2003

DoDI 8500.2, Information Assurance (IA) Implementation, February 6, 2003

DoD 8580.02-R, DoD Health Information Security Regulation, July 12, 2007

DoDI 4000.19, Interservice and Intragovernmental Support, August 9, 1995

TRICARE MANAGEMENT ACTIVITY
DATA SHARING AGREEMENT APPLICATION

APPENDIX D

EXAMPLE DATA FLOW (AS INDICATED IN SECTION 5A)

Data Flow Diagram – XYZ Company for DSAA #XX-XXXX "Analysis for TMA Leadership"