TRICARE Management Activity
Data Sharing Agreement Application

Internal Use Only
DSAA #:

The TRICARE Management Activity ("TMA") Privacy and Civil Liberties Office ("Privacy Office") conducts compliance reviews of requests for data owned and/or managed by TMA. This Data Sharing Agreement Application ("DSAA") is designed to assist in reviewing data requests for compliance with regulatory requirements, including Department of Defense ("DoD") Health Information Privacy Regulation (DoD 6025.18-R), which implements the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, and DoD Privacy Program (DoD 5400.11-R), which implements the Privacy Act of 1974, as amended. **Data access and extractions are handled through separate offices within the Military Health System ("MHS"), but prior approval of the data request is required by the Privacy Office.**

This application to request data must be completed by both the Applicant and the Government Sponsor, as defined below. Each will be asked to provide **initials** in order to certify the accuracy of a completed DSAA. Upon approval, this application will be incorporated into a Data Sharing Agreement ("DSA") that the Applicant, Government Sponsor, and Privacy Office Director must execute. Questions can be directed to DSA.mail@tma.osd.mil.

1. DATA REQUESTORS

a. Applicant:

The Applicant is the individual who will have primary oversight and responsibility for handling the data requested in this DSAA. See Appendix A for a full description of the Applicant's responsibilities.

- For contract-driven requests involving subcontractors, the Applicant must be an employee of the prime contractor.
- For projects with more than one prime contractor, a DSAA must be completed by **each prime contracting organization that will have custody of the requested data.**

Name & Title / Rank	**E-Mail Address**
Company / Organization	**Phone Number**
Mailing Address (Street, City, State, and Zip Code)	

b. Government Sponsor:

The Government Sponsor is the point of contact within TMA or the respective Armed Service who assumes responsibility for the contract, grant, agreement, or other project for which data is requested in this DSAA. See Appendix A for a full description of the Government Sponsor's responsibilities.

Name & Title / Rank	**E-Mail Address**
Company / Organization	**Phone Number**
Mailing Address (Street, City, State, and Zip Code)	

c. List the name(s) of each prime contracting organization and subcontracting organization that will have access to or use of the data requested:
Prime Contracting Organization(s) [including the Applicant, if applicable]:
Subcontracting Organization(s):

2. SOURCE OF THE DATA REQUEST

Contract / Grant / Cooperative Research and Development Agreement (CRADA) / Other Project Information:

Select the one below that forms the source of your data request:

- ☐ **Contract**
- ☐ **Grant**
- ☐ **CRADA**
- ☐ **List Other Project Type:** _____

Contract / Grant / CRADA / Other Project Number or Tracking Number (as applicable)	
Contract / Grant / CRADA / Other Project Name	
Current Option Year Period of Performance Dates	
Expiration Date of Contract / Grant / CRADA / Other Project	

Has standard Business Associate Agreement ("BAA") language been incorporated into the above-referenced contract, grant, CRADA, or other project documentation?

Standard BAA language is set forth at
http://www.tricare.mil/tma/privacy/downloads/2010630/Protected%20Business%20Associate%20Agreement.doc

☐ **Yes** ☐ **No**

If your response is "No" to the question above and the Privacy Office determines that this application is requesting or will provide access to data elements containing protected health information ("PHI"), you may be contacted and required to modify your contract, grant, CRADA, or other project documentation to incorporate BAA language before the application can be approved. PHI is defined in Appendix B.

3. PURPOSE OF THE DATA REQUEST

a. Explain in detail the purpose(s) of your data request. If your response exceeds the space available, please attach additional pages.

b. Do you intend to publish, report, or otherwise release any data, results, or findings related to this data request?	
☐ **Yes** ☐ **No**	
If "Yes," address the following two items:	**Set forth the precise type of data that will be published, reported, or otherwise released:** If your response exceeds the space available, please attach additional pages.
	Describe the method that will be used to ensure that there is minimal risk of identifying or re-identifying individuals: If your response exceeds the space available, please attach additional pages.

<u>Requirement</u>: For research requests that undergo review by an Institutional Review Board ("IRB"), any intent to publish, report, or otherwise release data, results, or findings must be included in materials submitted to that respective IRB for approval. The Government Sponsor is responsible for ensuring DoD requirements are met for publication/release.

4. DATA FLOW, USE AND MANAGEMENT

List, diagram, and/or otherwise describe the flow, use, and management of data from the time you receive the requested data through the duration of your above-noted contract, grant, CRADA, or other project. If your response exceeds the space available, please attach additional pages. If you respond by attaching a diagram / illustration, indicate below that your response will be attached.

5. FOR RESEARCH REQUESTS ONLY

Only complete this section if your data request is for research purposes: If your request does not pertain to research, skip this section and go to section 6 below.			
Name of Research Project if other than the name stated in section 2 above			
Principal Investigator			
Complete Mailing Address			
Telephone Number		**E-Mail Address**	
Has this project been reviewed by an IRB?			☐ **Yes** ☐ **No**
Has this research been reviewed by TMA's Exemption Determination and Secondary Review Officer? (Contact *DSA.mail@tma.osd.mil* with any questions)			☐ **Yes** ☐ **No**
Does this research involve a survey or information collection from ten (10) or more individuals?			☐ **Yes** ☐ **No**
If "Yes" to the previous question, indicate the type of approval below and provide the associated number and expiration date: ☐ **Report Control Symbol ("RCS")** ☐ **Office of Management and Budget ("OMB")**			**RCS / OMB Number:** **Expiration Date:**

6. SOURCE AND TYPE OF DATA REQUESTED

a. Indicate the system(s) owned and/or managed by TMA from which you are requesting data:

If you are not sure what systems contain the data that you need, contact DSA.mail@tma.osd.mil for assistance. See Appendix C for acronym listings of systems owned and/or managed by TMA.

☐ AHLTA	☐ M2	☐ TMDS
☐ CDM (from the MDR)	☐ MDR	☐ TOL
☐ CHCS	☐ MHS Learn	[space reserved]
☐ DMHRSi	☐ PDTS	
☐ EAS	☐ PEPR	
☐ Other systems (please specify):		

Requirement: Except for requests made by a health care provider for treatment purposes, all data requests must be limited to data elements that are minimally necessary to accomplish the intended purpose of the request.

b. Data Elements Requested from Systems Owned and/or Managed by TMA:

Check either or both options below that apply to your request.

☐	**To request specific data elements within a system:** Go to Data Request Templates at *http://www.tricare.mil/tma/privacy/Templates.aspx* to create a data element list specific to your contract, grant, CRADA, or other project. The most frequently used systems owned and/or managed by TMA will have a corresponding template. Use the default template entitled "General Data Request Template" for any system not otherwise listed. You must complete a template for *each* separate system indicated above from which you are requesting data. Within the template, you can select the data elements available for that system. After completing each applicable template, press the button to print out your data element list and attach it to this DSAA for submission. This DSAA will not be considered complete until you submit all applicable Data Request Templates.
☐	**To request all data elements within a system:** List each system below from which you are requesting "all data elements" and provide a detailed justification for this request. *Note: Requests for "all data elements within a system" should be avoided, whenever possible, and will be carefully scrutinized.* If your response exceeds the space available, please attach additional pages.

c. Select Type(s) of Data Receipt: Check options below that apply to the method in which you seek to receive the data requested, and fill in the requested information for the option(s) selected.	
☐	**Receive as an <u>extraction</u> (i.e., data will be physically removed from a system owned and/or managed by TMA and provided to the data requestors)** **Indicate the name of the MHS Office and/or its appointed designee that will prepare the extraction:** _____
☐	**Directly <u>access</u> via login (i.e., data requestors will directly log in to a system owned and/or managed by TMA)**

<u>Notice</u>: Based on the specific data elements that you request and any access you may have to systems owned and/or managed by TMA, as indicated by your responses to the above questions, the Privacy Office will determine the type/category of your data request under applicable privacy regulations. You are not asked to decide if your request meets the regulatory definitions of a limited data set, PHI, de-identified data and/or personally identifiable information ("PII") that excludes PHI. The Privacy Office will make this determination for you and will then review your request under the applicable privacy regulations. The Privacy Office will contact you if there are questions or issues that arise in making this determination.

d. Frequency of Extraction and/or Access (select one):	
☐	**One-time only**
☐	**Weekly**
☐	**Bi-weekly**
☐	**Monthly**
☐	**Quarterly**
☐	**Annually**
☐	**Other (please specify):**

7. DATA FROM NON-TMA SYSTEMS

a. Do you intend to merge, link, or otherwise associate requested data with data from any other sources outside of TMA?
☐ **Yes** ☐ **No**
If "Yes," explain why and how you will associate the requested data with data from non-TMA Systems: If your response exceeds the space available, please attach additional pages.

b. If "Yes" to 7a above, also indicate the non-TMA systems that you will be using in this regard and see the requirement noted below: See Appendix D for acronym listings of non-TMA systems.		
☐ DMDC	☐ PDHRA	☐ Other (please list):
☐ JTTR	☐ TRAC2ES	
☐ PDHA	[space reserved]	

Requirement: Be advised that you are required to obtain separate permission to use or disclose data from each of the respective non-TMA system owners and/or managers. The Privacy Office cannot approve data requests from these systems.

8. ADDITIONAL INFORMATION

To further assess privacy considerations, please respond to each of the following questions:	
Are you electronically collecting, maintaining, using, or disseminating PII? (PII is defined in Appendix B.)	☐ **Yes** ☐ **No**
Are you creating an item, collection, or grouping of information, in any media (e.g., paper and/or electronic), from which you will have the ability to retrieve the data by the name of an individual or some other personal identifier?	☐ **Yes** ☐ **No**

9. INFORMATION SYSTEM PROTECTION

a. Complete the following for each organization set forth in section 1c of this DSAA that will store, process, maintain, and/or use the requested data on an information system that has been granted a DoD Authorization to Operate ("ATO") or Interim Authorization to Operate ("IATO").

See Appendix B for the definition of an Accreditation Decision. If you are not sure, consult the Information Assurance Officer in your organization who has responsibility for the network(s) or server(s) you will be using to perform the work outlined in this data request.

Organization Name	System Name(s)	ATO or IATO	Expiration Date

b. List each organization set forth in section 1c of this DSAA that will store, process, maintain, and/or use the requested data on an information system that has not been granted an ATO or IATO and see the requirement noted below:

Requirement: A System Security Verification ("SSV") template must be completed by each organization indicated in section 9b above with respect to any information system on which it intends to store, transmit, process, or otherwise maintain the requested data that has not been granted an ATO or IATO.

The SSV template is available on the Privacy Office website link below. Please provide the completed SSV template(s), as required, with this DSAA.

http://www.tricare.mil/tma/privacy/downloads/FINAL_APPROVED_SSV_Locked.doc

10. APPLICABLE SUPPORTING DOCUMENTATION

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

☐ Data Flow, Use and Management Diagram/Illustration (see section 4)

☐ Data Request Template(s) for each system from which you are requesting data (see section 6b)

☐ SSV Template(s) (see section 9b)

☐ Other (briefly describe): _____

Requirement: You must submit all necessary and supporting documents before your DSAA is considered complete for processing.

11. CERTIFICATIONS

By electronically typing our initials in the respective boxes below, we certify that the information provided in this DSAA and all supporting documents is truthful and accurate. We understand that we are required to promptly notify the Privacy Office of any change(s) to this DSAA.

Applicant

_____

Printed Name and Rank/Title

_____

Date

☐ **By initialing here, I further certify that this application is submitted by me personally.**

Government Sponsor

_____

Printed Name and Rank/Title

_____

Date

☐ **By initialing here, I further certify that this application is submitted by me personally.**

Notice: The names and electronic initials above will be associated with the respective contact information provided in section 1 above and will be used for all communications by the Privacy Office related to this DSAA.

Internal Use Only

Other Related DSA Numbers: _____

Type of data request:
Based on data elements requested and level of access, if applicable. (see section 6)

- ☐ De-Identified pursuant to DoD 6025.18-R, C8.1
  Indicate method of de-identification:
  - ☐ Statistical Method; or
  - ☐ Safe Harbor Method
- ☐ Limited Data Set ("LDS") for the purpose of research, public health, or health care operations, pursuant to DoD 6025.18-R, C8.3
- ☐ PHI pursuant to DoD 6025.18-R, DL1.1.28
- ☐ PII pursuant to DoD 5400.11-R, DL1.14, *excluding PHI*

For PHI requests, purpose of the data request pursuant to DoD 6025.18-R (check all that apply):

- ☐ Research (C7.9), and confirm the following prerequisite approvals:
  - ☐ Exemption Determination and Secondary Review Officer approval received
  - ☐ TMA Privacy Board approval received, if applicable

☐ Treatment (C4.2)	☐ Judicial and Administrative Proceedings (C7.5)
☐ Healthcare Operations (C4.2)	☐ Avert a Serious Threat to Health or Safety (7.10)
☐ Payment (C4.2)	☐ Cadaveric Organ, Eye or Tissue Donation (C7.8)
☐ Required by Law (C7.1)	☐ About Decedents (C7.7)
☐ Public Health Activities (C7.2)	☐ Workers' Compensation (C7.12)
☐ Health Oversight Activities (C7.4)	☐ Specialized Government Functions (C7.11)
☐ Law Enforcement (C7.6)	☐ Victims of Abuse, Neglect, or Domestic Violence (C7.3)

Has required BAA language been incorporated? (see sections 2 and 3a)	☐ **Yes**	☐ **No**	☐ **N/A**
Are required SSV templates approved? (see section 9)	☐ **Yes**	☐ **No**	☐ **N/A**
Is there intent to publish, report, or otherwise release data? (see section 3b)	☐ **Yes**	☐ **No**	☐ **N/A**
Has a Privacy Impact Assessment been reviewed? (see section 8)	☐ **Yes**	☐ **No**	☐ **N/A**
Is a System of Records (SOR) Notice needed for a new SOR? (see section 8)	☐ **Yes**	☐ **No**	☐ **N/A**
Has a Privacy Act Statement been reviewed? (see section 8)	☐ **Yes**	☐ **No**	☐ **N/A**
Does the data request invoke the need for a Computer Matching Agreement? (see sections 2 and 7)	☐ **Yes**	☐ **No**	
Does the data request invoke the need for an agreement with DoD Quality Management Programs? (see section 3)	☐ **Yes**	☐ **No**	

Applicable SORN Number(s):_____

This DSAA is Approved by signing below:

Signature:_____ Date: _____
Data Sharing Compliance Officer, TMA Privacy and Civil Liberties Office

APPENDIX A

Responsibilities

Applicant / Recipient responsibilities are as follows:

- Agree to and execute a DSA after the DSAA is reviewed by the Privacy Office
- Provide and maintain accurate and complete responses to the DSAA and promptly notify the Privacy Office of any change(s)
- Maintain current information with the Privacy Office and, if necessary, complete a DSA – Change of Applicant / Recipient template to reflect any transition within fifteen (15) days
- When a change is required to an executed DSA (which incorporates an approved DSAA), promptly submit to the Privacy Office the appropriate template(s): DSA – Renewal Request, DSA – Modification Request, or DSA – Extension Request
- Safeguard the integrity of the data received and comply with all applicable standards for protecting its privacy and security
- Ensure 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 at *http://www.tricare.mil/tma/privacy/breach.aspx*
- Adhere to BAA requirements, if applicable
- Submit a completed and signed DSA – Certification of Data Disposition to the Privacy Office within thirty (30) days of the expiration of the DSA or the date of notification that the data are no longer necessary, *whichever comes first*

Government Sponsor responsibilities are as follows:

- Agree to and execute a DSA once the DSAA is reviewed by the Privacy Office
- Confirm and/or provide accurate and complete responses to the DSAA and promptly notify the Privacy Office of any change(s)
- Maintain current information with the Privacy Office and, if necessary, complete a DSA – Change of Government Sponsor template to reflect any transition within fifteen (15) days
- When a change is required to an executed DSA (which incorporates an approved DSAA), ensure the appropriate template(s) is promptly submitted to the Privacy Office: DSA – Renewal Request, DSA – Modification Request, or DSA – Extension Request
- Ensure compliance with applicable standards for protecting the privacy and security of the data received
- Ensure 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 at *http://www.tricare.mil/tma/privacy/breach.aspx*
- Ensure adherence to BAA requirements, if applicable
- Ensure that a completed and signed DSA – Certification of Data Disposition is submitted to the Privacy Office within thirty (30) days of the expiration of the DSA or the date of notification that the data are no longer necessary, *whichever comes first*
- Oversee the work performed by the Applicant / Recipient for the duration of the DSA
- Ensure that the publication or release of any data, results, or findings adheres to applicable DoD requirements

APPENDIX B

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"). The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD Public Key Infrastructure-certified digital signature. [DoDI 8500.1, DoD Information Assurance Certification and Accreditation Process ("DIACAP"), E2.2.]

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.

APPENDIX C

Acronyms for Systems Owned and/or Managed by TMA

CDM	Clinical Data Mart
CHCS	Composite Health Care System
DMHRSi	Defense Medical Human Resources System - internet
EAS	Expense Assignment System
M2	Management Analysis and Reporting Tool
MDR	MHS Data Repository
MHS Insight	Military Health System Insight
MHS Learn	Military Health System Learn
PDTS	Pharmacy Data Transaction Service
PEPR	Patient Encounter Processing & Reporting
TOL	TRICARE Online
TMDS	Theater Medical Data Store

APPENDIX D

Acronyms for Non-TMA Systems

DMDC	Defense Manpower Data Center
JTTR	Joint Theater Trauma Registry
PDHA	Post Deployment Health Assessment
PDHRA	Post Deployment Health Reassessment
TRAC2ES	Transportation Command ("TRANSCOM") Regulating and Command & Control Evacuation System