DATA SHARING AGREEMENT FOR PROTECTED HEALTH INFORMATION

The Applicant and Government Sponsor, as identified and defined in the Data Sharing Agreement Application ("DSAA"), enter into this Data Sharing Agreement ("DSA") with TRICARE Management Activity ("TMA"). The purpose of this DSA is to ensure compliance with applicable regulatory requirements, including the Privacy Act of 1974 as amended (5 USC § 552a), implemented through Department of Defense ("DoD") Privacy Program (DoD 5400.11-R), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule and Security Rules (45 CFR Parts 160 and 164, Subparts A and C), implemented through DoD Health Information Privacy Regulation (DoD 6025.18-R) and DoD Health Information Security Regulation (DoD 8580.02-R) respectively.

1. **DSA #09-595B "I. BIHR, II. MILCO, III. DHR".** Based on data elements set forth in the Data Request Templates and/or the Applicant's requested level of access to systems owned and/or managed by TMA, the TMA Privacy and Civil Liberties Office ("Privacy Office") has determined that your request is for **Protected Health Information** ("PHI") as defined by the HIPAA Privacy Rule at 45 CFR §160.103 and DoD 6025.18-R at DL1.1.28. The aforementioned DSAA is hereby approved and the Applicant is hereinafter referred to as the "Recipient". The Recipient acknowledges and understands that:

   a. The above-referenced DSAA set forth as **Attachment A**, including all applicable Data Request Templates, is hereby incorporated by reference and all information contained in the DSAA is relied upon in executing this DSA.

   b. Data needed for your contract, grant, Cooperative Research and Development Agreement ("CRADA"), or other project that is not owned and/or managed by TMA will require separate permission from each of the respective non-TMA system owners and/or managers.

2. **Scope.** The Recipient seeks to receive PHI from TMA for the sole purpose as set forth in the DSAA. The parties acknowledge and recognize that this DSA only pertains to the Privacy Office's compliance review of the data requested by the Recipient. This DSA does not authorize access to or otherwise provide an extraction of the requested data. Access to or extraction of data is handled through separate offices within the Military Health System.

3. **Minimum Necessary Information.** The Recipient represents that the data requested is limited to only that which is minimally necessary to accomplish Recipient's purpose as set forth in this DSA and in the DSAA (**Attachment A**).

4. **Obligations of Recipient.** The Recipient agrees to the following:

   a. Not to use or further disclose the information other than as permitted by this DSA or as otherwise required by law.

b. Use appropriate administrative, technical, and physical safeguards to protect the confidentiality of the PHI and to prevent use or disclosure of the information other than as provided by this DSA.

c. Promptly report to the Privacy Office any use or disclosure of the information not provided for by this DSA of which it becomes aware and take reasonable steps to limit any further use or disclosure.

d. Ensure that any agents, including subcontractors, to whom the Recipient provides the data agree to the same restrictions and conditions that apply to the Recipient with respect to such information.

5. **Research-Related Contracts / Grants / CRADAs / Other Projects.** For research-related requests, the Recipient acknowledges and agrees to adhere to all requirements as set forth by the TMA Privacy Board.

6. **Responsibilities of Recipient and Government Sponsor.** Recipient, referred to as "Applicant" in the DSAA, and Government Sponsor are required to comply with the responsibilities set forth in Appendix A of the DSAA which is included as **Attachment A**.

7. **Limitation of Use and Disclosure.** The Recipient must not use, disclose, market, release, show, sell, rent, lease, loan, or otherwise grant access to the data specified in this DSA, except as expressly permitted herein or otherwise required by law.

8. **Reporting Requirements.** The Recipient must promptly provide notice of any actual or possible breach, including any use or disclosure of the information not provided for by this DSA of which it becomes aware. A breach is defined as an actual or possible loss of control, unauthorized disclosure of, or unauthorized access to, personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes and where one or more persons will be adversely affected. Recipient agrees to follow breach reporting requirements as established by the DoD 5400.11-R and the OSD Memorandum "Safeguarding Against and Responding to the Breach of PII" which can be found at http://www.tricare.mil/tma/privacy/breach.aspx. If an actual or possible compromise of data occurs, the event must be treated as a breach and the following two notices are required: (1) Within one hour of discovery of an actual or possible breach, the Recipient must complete and submit the online notice form at http://www.us-cert.gov and, (2) Within 24 hours of discovery, the Recipient must complete the TMA Breach Report Form and email the form to PrivacyOfficerMail@TMA.osd.mil or report by phone at (703) 681-7500. Breaches that are otherwise subject to notification and reporting requirement under Section 13402 of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") will be addressed by the Privacy Office.

9. **Effective Date, Retention/Expiration Date, and Termination.**

   a. **Effective Date and Retention/Expiration Date.** This DSA becomes effective upon signature by the Director, Privacy Office ("Effective Date"). It will remain in force, and all data subject to this DSA, unless renewed, may be retained for: (i) one (1) year; *or*, (ii) until the end of the contract period of performance, whichever comes first. The DSA expiration date is April 1, 2013.

   b. **Termination for Cause.** Upon knowledge of a material breach by the Recipient, the Privacy Office reserves the right to terminate this DSA immediately.

   c. **Effect of Expiration or Termination.** The Recipient agrees to promptly notify the Privacy Office when its use of the data is no longer necessary, if such use is completed before the Retention/Expiration Date. The Recipient further agrees to submit a completed DSA – Certification of Data Disposition template, available on the Privacy Office's Website at http://www.tricare.mil/tma/privacy/Templates.aspx, within thirty (30) days of the Retention/Expiration Date or the date of notification that the data are no longer necessary, *whichever comes first*.

10. **Certification of Data Disposition.** The Recipient agrees to dispose of all electronic and hard copy data, including derivative data and data in the possession of any business associate(s), agent(s), or subcontractor(s) as specified in the subsections below and set forth in the DSA – Certification of Data Disposition. Should Recipient indicate that there are no data for disposition, Recipient understands that it will be required to certify that no data, including derivative data, were ever downloaded or maintained locally in any form or format by a business associate, agent, or subcontractor or were ever printed in hard copy. The Recipient agrees not to retain TMA data or any parts thereof, after the data are disposed of and a completed DSA – Certification of Data Disposition is received by the Privacy Office.

    a. **Data Destruction.** Recipient agrees to shred or burn hard copy files/data and to overwrite, degauss (i.e., demagnetize), and/or physically destroy electronically stored media. [Note: Clearing data (i.e., deleting files) is not an approved method of sanitizing electronic storage media.]

    b. **Data Return.** Recipient is required to return data to TMA, if it receives specific written instruction for data return.

    c. **Data Transfer.** Recipient may transfer data to another executed DSA only upon prior approval by the Privacy Office.

11. **Modification, Renewal and Extension.**

    a. **Modification.** This DSA may be modified at any time, as necessary, by completing the DSA – Modification Request template available on the Privacy Office's website at http://www.tricare.mil/tma/privacy/Templates.aspx. Any such modifications shall not alter

the Effective Date or Retention/Expiration Date, unless such modification requires a new DSAA and DSA.

b. **Renewal.** This DSA may be renewed annually, as necessary, by completing the DSA – Renewal Request template available on the Privacy Office's website at http://www.tricare.mil/tma/privacy/Templates.aspx. This DSA will automatically renew annually provided that a renewal request is approved by the Privacy Office.

c. **Extension.** An extension of a previously executed DSA may be requested by completing the DSA – Extension Request template available on the Privacy Office's website at http://www.tricare.mil/tma/privacy/Templates.aspx. This DSA will automatically extend to the period indicated in the template, upon approval of the DSA – Extension Request.

12. **Compliance with Laws.** As applicable, all parties to this DSA are equally responsible for ensuring that the data are protected in accordance with all applicable privacy and security laws, including the Privacy Act of 1974, HIPAA, HITECH Act, the E-Government Act of 2002, Title III, and the Federal Information Security Management Act. Any parties that are components within DoD are likewise responsible for adherence to any and all applicable and associated DoD implementation regulations or issuances.

13. **Ambiguity.** Any ambiguity in this DSA shall be resolved to permit TMA to comply with the laws and regulations outlined in Section 12.

The undersigned individuals hereby attest that they are authorized to enter into this DSA on behalf of their respective organizations and agree to all the terms specified herein. The Recipient and Government Sponsor understand that this DSA is binding upon and will inure to the benefit of the Recipient and Government Sponsor and their respective successors and/or assignees.

Applicant / Recipient

C J Phillips — 7 MAY 2012

Signature — Date

Chris Phillips, MD, MPH

Printed Name

Senior Epidemiologist

Rank/Title

Government Sponsor

5/7/12 (for Dr Crum)

Signature — Date

Nancy F. Crum, MD, MPH

Printed Name

Director, DoD Center for Deployment Health Research (NHRC)

Rank/Title

TMA Privacy and Civil Liberties Office

THOMAS.LINDA.SKILES.1410880209

Digitally signed by THOMAS.LINDA.SKILES.1410880209
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=TMA, cn=THOMAS.LINDA.SKILES.1410880209
Date: 2012.05.08 08:59:16 -04'00'

5/8/12

Director, TMA Privacy and Civil Liberties Office
5111 Leesburg Pike, Suite 810
Falls Church, VA 22041
Phone: 703-681-7500

Date ("Effective Date")

ATTACHMENT A
Data Sharing Agreement Application,
Including All Applicable Data Request Templates

TRICARE Management Activity
Data Sharing Agreement Application

Internal Use Only
DSAA #:
09-595.1B, .2B, .3B

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**
Chris Phillips, MD, MPH / Senior Epidimiologist	chris.phillips@med.navy.mil
Company / Organization	**Phone Number**
Henry M. Jackson Foundation	619-553-7729
Mailing Address (Street, City, State, and Zip Code)	
140 Sylvester Road, San Diego, CA 92106-3521	

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**
Nancy F. Crum, MD, MPH / Director	nancy.crum@med.navy.mil
Company / Organization	**Phone Number**
DOD Center for Deployment Health Research, NHRC	619-553-7335
Mailing Address (Street, City, State, and Zip Code)	
140 Sylvester Road, San Diego, CA 92106-3521	

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]: Henry M. Jackson Foundation
Subcontracting Organization(s): None

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)	N66001-04-D-2506/009
Contract / Grant / CRADA / Other Project Name	I. BIHR, II. MILCO, III. DHR
Current Option Year Period of Performance Dates	9/26/11 - 3/25/12
Expiration Date of Contract / Grant / CRADA / Other Project	3/25/12

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.

I. National Surveillance for Birth Defects Among Department of Defense (DoD) Health Care Beneficiaries - The Birth and Infant Health Registry (BIHR) = To establish a surveillance program for birth defects among Department of Defense Health Care Beneficiaries. Such a registry will provide baseline data, assist with medical surveillance, and gather statistics about reproductive outcomes. The primary objective establishes surveillance for major birth defects among DoD beneficiary infants and provide annual prevalence data on birth defects diagnosed in infancy, beginning with all military infants born in 1998.

In support of the recommendations of the United States Senate Committee on Veterans' Affairs. the Institute of Medicine's Committee to Review the Health Consequences of Service During the Persian Gulf War. and the Presidential Advisory; Committee on Gulf War Veterans' Illnesses. This DoD registry concept has been endorse by the Surgeons General of the US Army, Navy and Air Force. and by DoD/HA. (See attachment, Statement of DoD-HA Policy from Dr. Sue Bailey for BIHR.)

II. Prospective Study of U.S. Military Forces: The Millennium Cohort Study (MILCO) = To determine how the health of US military veterans change over time. and to determine the health impact of military deployments upon the adjusted incidence of chronic disease and serve as the foundation for a portfolio of future studies of the impact of military service. Including anthrax vaccination, on the health of members of the armed forces.
See also http://www.millenniumcohort.org.

This study was designed in response to the Institute of Medicine's report "Measuring Health" and funded by DoD/HA. The study designed has been favorably reviewed by the American Institute of Biological Sciences (AIBS). (See attachment, IOM Report Executive Summary. Measuring Health.pdf)

III. Deployment Health Research (DHR) = To conduct epidemiological studies investigating the health experience of military personnel and their families. Studies focus on frequency of symptoms, hospitalizations, reproductive outcomes, risks for autoimmune disorders, cancer risk factors and surveillance, mental health outcomes, mortality and other health outcomes among DoD beneficiary populations, both military and civilian.

Section 743 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 authorized the Secretary of Defense to establish a center devoted to " ...longitudinal study to evaluate data on the health conditions of members of the Armed Forces upon their return from deployment ... " On September 30, 1999, the Assistant Secretary of Defense for Health Affairs executed Section 743 to establish the DoD Center for Deployment Health Research, designated to have remote access to personnel and health data maintained by all DoD organizations.

For all three protocols above, SSN, EDIPN, Date of Birth, and Gender codes are required to link data from key tables in the MDR (SADR, SIDR, HCSR-I, HCSR-NI. TED, DEERS, Pharmacy, Laboratory. Radiology). The DDS, FMP and other Family Relationship codes to confirm familial relationships for the BIHR and MILCO.

Studies include investigations of personnel who remain on active duty and personnel who have left military service, as well as their families. Records are collected and assembled to permit investigative examination and analysis of reports of possible exposure to biological, chemical, radiological, disease, or environmental agents incident to service in military deployments or related operations, exercises, or tests, to conduct scientific or related studies or medical follow-up programs, and to assist in the resolution of deployment related issues. All studies conducted at the DoD. Center for Deployment Health Research are conducted using protocols that are approved by the Naval Health Research Center, and other appropriate Institution Review Boards.

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.

Identifiable data will not be disclosed or reused, and will only be used to meet the stated study objectives.

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.

Only the minimal amount of data needed to accurately identify an individual will be used, this is usually the EDIPN or the combination of gender, ssn, and dob. Aggregate data and post analysis results for publication will NEVER include any PHI. Results which have the potential to identify any individual by identifiers other than EDIPN, gender, ssn, or dob will be not be reported in aggregate tables.

<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.

PHI data, to include SSN, EDIPN, Date of Birth, Gender, FMP, DDS, Family Relationship codes are required to link data from core MDR tables, aka the "pub" tables (SADR, SIDR, HCSR-I, HCSR-NI, TED, DEERS, Pharmacy, Laboratory, Radiology). In addition, the personal identifiers are required to link MDR data with MILCO survey data and declassified deployment history data.

For BIHR, a birth defect case will be defined as a DoD beneficiary birth with a date of birth, on or after January 1, 1998, and a congenital anomaly diagnosis that is classified as a birth defect by the CDC. This selection of birth defects is a standard for US state birth defects registries. It includes diagnoses (ICD-9 codes) that are defined as structural, or adversely affecting an individual's health functioning or social acceptability; and diagnosed before a child's first birthday.

For MILCO, the prospective methodology will permit the accurate description of the incidence and natural history of medical conditions in this population. Most importantly, the impact of future deployments will be captured and addressed by determining whether conditions brought to medical attention post-deployment represent new occurrences or pre-deployment health states. The data from the survey will not be weighted, and findings from all subgroups will be reported. Baseline healthcare data and exposure history obtained from the survey will be joined to deployment history data and DoD healthcare utilization data (using ICD-9, CPT codes) to study any associations and/or interactions from baseline health status, exposure history, deployment history and health outcomes.

For DHR, personal identifiers are required to link data with recruit assessments, deployment history data and medical outcomes, with emphasis on mental health to include PTSD, TBI, and for cancer surveillance and risk factors.

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	I. BIHR, II. MILCO, III. DHR		
Principal Investigator	Nancy Crum, MD, MPH		
Complete Mailing Address	140 Sylvester Road, San Diego, CA 92106-3521		
Telephone Number	619-553-7335	**E-Mail Address**	nancy.crum@med.navy.mil

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")** = MILCO ☐ **Office of Management and Budget ("OMB")**	**RCS / OMB Number:** DD-HA(AR)2106 **Expiration Date:** 1/31/13

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. Core files in "pubs" (All fields/All years) - SIDR, SADR, Ancillary HCSRN, HCSRI, DEERS, TEDN, TEDNI, Death, PDTS, NMOP. Login via non OOB account to: program in SAS, start jobs, monitor job completion status.

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):** Continuous "ad hoc" access via SAS Sessions as needed, approximately twelve sessions per month.

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. For DMDC active duty rosters are used to create accurate denominators for deployment health research and to verify, by month, active duty status. Database joins to these DMDC files by either EDIPN or the combination of gender, ssn and dob. For JTTR, PDHA, PHDRA; these databases are also important data sources for deployment health research. Database joins to these files are by EDIPN (if populated) or the combination of gender, ssn and dob.

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
Henry Jackson Foundation	Naval Medical Center San Diego (NMCSD) Local Area Network (LAN)	ATO	2/28/2014

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:

None

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

Chris Phillips, MD, MPH / Senior Epidemiologist, Henry M. Jackson Foundation, NHRC

Printed Name and Rank/Title

March 12, 2012

Date

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

Government Sponsor

Martin R. White for Nancy Crum, MD, MPH / Director DoD Center for Deployment Health Research, NHRC

Printed Name and Rank/Title

March 12, 2012

Date

MRW **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)
- ☐ Healthcare Operations (C4.2)
- ☐ Payment (C4.2)
- ☐ Required by Law (C7.1)
- ☐ Public Health Activities (C7.2)
- ☐ Health Oversight Activities (C7.4)
- ☐ Law Enforcement (C7.6)
- ☐ Judicial and Administrative Proceedings (C7.5)
- ☐ Avert a Serious Threat to Health or Safety (7.10)
- ☐ Cadaveric Organ, Eye or Tissue Donation (C7.8)
- ☐ About Decedents (C7.7)
- ☐ Workers' Compensation (C7.12)
- ☐ Specialized Government Functions (C7.11)
- ☐ 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): DHA 07

This DSAA is Approved by signing below:

Signature: RCDuShuldS **Date:** 5/2/12

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