The purpose of this presentation is to:

- Provide an overview of the DHA Privacy and Civil Liberties Office (Privacy Office) Data Sharing Program, as it relates to research including:
  - The Privacy Office's use of the Data Sharing Agreement (DSA)
  - The parties involved in the DSA Process
  - How the Privacy Office utilizes the DSA Application (DSAA) and DSA-related supporting documentation
The DSA process allows the Privacy Office to:

- Confirm that **DHA data** will be used or disclosed in compliance with:
  - DoD Privacy Program (DoD 5400.11-R), which implements the Privacy Act of 1974, as amended
  - DoD Health Information Privacy Regulation (DoD 6025.18-R), which implements the HIPAA Privacy Rule
  - DoD Health Information Security Regulation (DoD 8580.02-R), which implements the HIPAA Security Rule
  - DoD Instruction 8582.01, “Security of Unclassified DoD Information on Non-DoD Information System”

- DHA is defined as personal information, including health information, maintained on a DHA managed system, as documented in the Defense Health Program System Inventory Reporting Tool (DHP SIRT) *Currently under Office of General Council (OGC) review*
Data Sharing Program Overview
The Privacy Office's use of the DSA

The DSA is as an *administrative control measure*, used to:

- Confirm that DHA data will be used as permitted or required
- Exercise administrative, technical and physical safeguards to protect the privacy of PHI, as required by HIPAA
- Determine the HIPAA-defined category of data intended for use (i.e., PHI, a limited data set, or de-identified PHI)
  - HIPAA permits a covered entity to use or disclose a limited data set (LDS) for research, public health, or health care operations purposes
    - If the covered entity enters into a data use agreement (DUA) with the data recipient
- Maintain records to confirm compliance in case of an investigation
“Data Sharing Agreements” is an *umbrella term*, used by the Privacy Office, when referring to the following agreements:

- A DSA for Protected Health Information (PHI)
- A DSA for Personally Identifiable Information (PII) excluding PHI
- A DSA for De-Identified Information
- A DUA for a LDS
Data Sharing Program Overview

Parties involved in the DSA Process include:

- **The DHA Privacy Office**: performs a compliance review to determine whether the intended data use complies with all applicable requirements.

- **The DHA Privacy Board**: reviews proposed research-specific uses of DHA PHI to confirm that the data will be used in compliance with HIPAA research requirements.

- **The System Program Office**: approves access to DHA data systems, and has the final say as to the feasibility of obtaining DHA data from a system within their area of responsibility.

- **The DSA Requesting Parties**: for research-related purposes, the requesting parties may include both non-DoD researchers and government personnel.
The DSA Government Sponsor

- The point of contact (civilian or uniformed Service member) from within the covered entity's sponsoring organization
  - Assumes *overall* responsibility, on behalf of the government, for the projected data use and protection
  - Confirms that the information provided in the DSAA is accurate


Data Sharing Program Overview
The parties involved in the DSA Process

The DSA Applicant/Recipient

■ The individual who has primary responsibility for safeguarding the DHA data during its expected use

☐ If non-DoD support is involved (i.e., contractor or non-DoD grant recipient) the Applicant be an employee of the primary supporting organization

☐ Even when a project involves subcontractors, and the data is solely handled by those subcontractors

☐ When a project’s data use involves more than one primary contractor or grant recipient organization, a DSAA must be completed for each primary organization that requires data for the project

☐ The Applicant is referred to as the Recipient in the executed DSA
What is a DSAA?

- The DSAA is an application, designed by the Privacy Office, to prompt data requestors to accomplish the following objectives before a DSA will be executed:

  - Make reasonable efforts to verify that DHA data are limited to the minimum necessary for achieving the intended purpose
  - Obtain satisfactory assurance that the DHA data will be appropriately safeguarded
  - Verify that the use of DHA data is permitted by the responsible DHA system program office
Data Sharing Program Overview
How the Privacy Office utilizes the DSAA and supporting documentation

The DSAA also allows the Privacy Office to confirm the following key compliance points:

- DHA data will be used according to the permitted uses defined in the applicable System of Records Notice (SORN)
- Information system(s) and networks, intended for data processing and/or storage, have appropriate safeguards
- Research-related data uses have been reviewed by the applicable compliance offices, and have obtained the respective determinations, including:
  - Institutional Review Board (IRB)
  - DHA Human Research Protection Program (HRPP)
    - When DHA data will be used for research purposes, and the protocol was not reviewed by a primary IRB within DoD
  - DHA Privacy Board
Data Sharing Program Overview
How the Privacy Office utilizes the DSAA and supporting documentation

Research-related DSAAAs

- Include the following information on the DSAA, as appropriate:
  - The DHA HRPP determination reference number and expiration date, if the protocol was *not* reviewed by a primary IRB within DoD
  - The survey license number and expiration date, if the data will be used for survey purposes

- DSAAs submitted for research involving the use of PHI, greater than LDS, will be forwarded to the DHA Privacy Board for review

- DSAAs may be reviewed concurrently with other research-specific compliance reviews (i.e., Privacy Board, DHA HRPP)
A completed SSV is required when data will be stored, transmitted, processed, or otherwise maintained on an information system that has not been granted a DoD Authority to Operate (ATO) or Interim Authority to Operate (IATO) in order to review for compliance with DoD 8580.02-R, DoD Health Information Security Regulation” and DoDI 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems”
Data Request Templates (DRTs)

- The Privacy Office created 3 separate DRTs to help DSA Applicants and Government Sponsors list the data elements needed for the project or study
  - The DRT for MHS Data Repository *(MDR) Extractions*
  - The *General* DRT (for extractions from all other DHA systems)
  - The DRT for *Access by Login* (to use for any DHA System)

- If the data elements are already listed on another document, and can be provided to support the DSAA, a separate DRT is not necessary
Data Sharing Program Overview
How the Privacy Office utilizes the DSAA and supporting documentation

Final Steps

- After the DSAA is approved by the Data Sharing Compliance Manager:
  - The appropriate DSA will be sent to the Recipient (reflected as the Applicant on the DSAA) and the Government Sponsor for signature
  - Once the Recipient and Government Sponsor sign and return the DSA, the Privacy Office will provide final signature
  - The executed DSA, incorporating the approved DSAA, will be sent to the Recipient and Government Sponsor for their records
When the expiration date approaches, a request to renew the executed DSA may be submitted to the Privacy Office if:

- There are no substantive changes to the data use, as described in the approved DSA
- The project or contract has not ended

If the data use, as described in the approved DSAA, changes:

- A DSA modification request template should be completed and submitted to the Privacy Office for review and approval
- Examples of changes that need to be submitted for review include staff changes and changes to risk level (i.e., exempt to minimal risk, etc.)
Data Sharing Program Overview
How the Privacy Office utilizes the DSAA and supporting documentation
Data Sharing Program Overview
Additional DSA-Related Information

Additional Slides
De-identified PHI excludes all 18 categories of HIPAA identifiers:

1. Names
2. All geographic subdivisions smaller than a State, except for the initial three digits of a zip code if:
   a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people
   b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, and all ages over 89 - except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers including fingerprint and voiceprints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code except as permitted

A limited data set is PHI that excludes 16 of the 18 categories of HIPAA identifiers:

1. Names
2. Address other than town, city, state, zip code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Account numbers
9. Health plan beneficiary numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web URLs
14. IP address
15. Biometric identifiers, including fingerprint and voiceprints
16. Full-face photographic images and comparable images
Data Sharing Program Overview
Additional DSA-Related Information

Use the chart below to determine the appropriate office to direct specific inquiries:

<table>
<thead>
<tr>
<th>DHA Data Sharing Program</th>
<th>Support Agreements Manager (SAM) Office</th>
<th>Appropriate System Program Office</th>
<th>DHA HRPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA &amp; DSAA completion/coordination</td>
<td>Support Agreement coordination</td>
<td>Data access/extraction coordination</td>
<td>Protocol compliance review coordination</td>
</tr>
<tr>
<td><strong>Determination of Data-Category</strong></td>
<td>Choosing the appropriate Support Agreement:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Personally identifiable information (PII) excluding PHI</td>
<td>✓ Interagency Agreement</td>
<td>Confirmation that data maintained in a specific system may be used for the requested purpose</td>
<td></td>
</tr>
<tr>
<td>✓ PHI</td>
<td>✓ Memorandum of Understanding (MOU)</td>
<td></td>
<td>Confirmation that the protocol involves research as defined by the Common Rule</td>
</tr>
<tr>
<td>✓ LDS</td>
<td>✓ Memorandum of Agreement (MOA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ De-identified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>General Data Sharing questions/guidance</strong></td>
<td><strong>General Support Agreements questions/guidance</strong></td>
<td><strong>General system-specific questions/guidance</strong></td>
<td><strong>General research questions/guidance</strong></td>
</tr>
</tbody>
</table>
Data Sharing Program Overview
Additional DSA-Related Information

Defense Health Clinical Systems (DHCS):

Defense Health Services Systems (DHSS):

Support Agreements Manager (SAM) e-mail:
SupportAgreements@dha.mil

Contract language & Privacy clauses:
http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties/Privacy-Contract-Language

Systems of Record Notices (SORNs):
http://dpcld.defense.gov/Privacy/SORNs.aspx

Department of Health & Human Services (HHS) HIPAA De-identification Guidance:

DoD 6025.18-R, DoD Health Information Privacy Regulation:

DoD 8580.02-R, DoD Health Information Security Regulation: