Defense Health Agency
Data Sharing Agreement Application

Table of Contents

Click a heading below to advance directly to the desired DSAA section:

PROJECT TILE	SECTION 1, Page 2
CONTACT INFORMATION	SECTION 2, Page 2
SUPPORT ARRANGEMENTS	SECTION 3, Page 3
PROJECT DESCRIPTION / JUSTIFICATION FOR DATA USE	SECTION 4, Page 3
DATA DE-IDENTIFICATION, PUBLISHING AND REPORTING	SECTION 5, Page 4
DATA FLOW, USE AND MANAGEMENT	SECTION 6, Page 5
RESEARCH REQUESTS	SECTION 7, Page 6
SOURCE AND TYPE OF DATA	SECTION 8, Page 7
ADDITIONAL INFORMATION	SECTION 9, Page 8
SYSTEM SECURITY INFORMATION	SECTION 10, Page 8
APPLICABLE SUPPORTING DOCUMENTATION	SECTION 11, Page 8
CERTIFICATIONS	SECTION 12, Page 9
RESPONSIBILITIES	APPENDIX A, Page 10
DE-IDENTIFIED, SENSITIVE AND PROPRIETARY DATA	APPENDIX B, Page 11
EXAMPLE DATA FLOW	APPENDIX C, Page 12
BUSINESS ASSOCIATE FUNCTIONS AND SERVICES	APPENDIX D, Page 13
DEFINITIONS, ACRONYMS AND REGULATORY REQUIREMENTS	APPENDIX E, Page 14

Defense Health Agency
Data Sharing Agreement Application

The Data Sharing Agreement Application (DSAA) is designed to assist the Defense Health Agency (DHA) Privacy and Civil Liberties Office (Privacy Office) with its consideration of prospective data uses involving DHA data. Each application is reviewed to confirm that the potential data use, described therein, complies with the applicable privacy and security regulatory requirements.

Both the Applicant and the Government Sponsor, defined below, must complete this application. 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 referenced. Upon approval, this application will be incorporated into a Data Sharing Agreement (DSA).

The Privacy Office neither grants system access, nor provides data extractions; however, prior to gaining access to, or an extraction of the data, the appropriate program office may require an executed DSA.

See Appendices A - E for applicable requirements, responsibilities, definitions, acronyms, and examples.

1. PROJECT TITLE

2. CONTACT INFORMATION

a. **Applicant:** *See Appendix A for a full description of responsibilities*
If contractors will access the data, the Applicant must be from the primary contracting organization.

(i) Indicate the type of Applicant:

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

(ii) Enter Applicant's Professional Contact Information:

Applicant Name		Title or Rank	
Company or Organization		Street Address	
City	State	Zip	Country
Phone Number		E-mail Address	

b. **Government Sponsor :** *See Appendix A for a full description of responsibilities*

(i) Enter Government Sponsor's Professional Contact Information:

Government Sponsor Name		Title or Rank	
Office or Agency		Street Address	
City	State	Zip	Country
Phone Number		E-mail Address	

3. SUPPORT ARRANGEMENTS

a. Select the type of arrangement under which this project was awarded, and provide the arrangement number:

☐ Contract ☐ Grant ☐ Cooperative Research and Development Agreement (CRADA)

☐ Other: *Describe any other type of arrangement, or if support arrangement is not applicable (i.e. government only)*

b. Support Arrangement Number, *if applicable:*

c. Period of Performance (PoP) Dates:
(*Not supported by contract? List expected start and completion dates.)*

PoP Start: PoP End:

d. Other Primary Contractors: (*Each primary contracting organization using the data is required to submit a separate DSAA)*

e. Subcontracting Organizations

(i) List each subcontracting organization that will have access to or use of the data:

(ii) Briefly describe how subcontractor(s) will use the data:

f. The support arrangement referenced above includes business associate agreement language: ☐ Yes ☐ No
If this data use involves PHI, a modification to incorporate business associate language into the support arrangement may be required before the DSAA is approved. Language may be found on the Privacy Office website

4. PROJECT DESCRIPTION / JUSTIFICATION FOR DATA USE

Describe the intended data use, including a justification of why the data are needed.
If this response exceeds the space available, attach additional pages.

5. DATA DE-IDENTIFICATION, PUBLISHING AND REPORTING

a. If the use or storage of data involves variables that have been de-identified according to DoD 6025.18-R, complete this section; otherwise, skip to section 5b. (*See Appendix B for more information)*

(i) Indicate the intended de-identification method:

☐ Expert Determination ☐ Safe Harbor ☐ Combination (Expert Determination & Safe Harbor)

(ii) Describe data de-identification steps (i.e., encryption, redaction, small cell size eradication):

(iii) Indicate the parties who intend to de-identify the data, and list their HIPAA defined qualifications:

(iv) Justify any use of proprietary and sensitive data (e.g., pharmacy dispensing/ingredient cost):

(v) If applicable, list any remaining identifiers associated with the 18 HIPAA categories of PHI:

b. Publishing, Reporting or Other Data Release

(i) Describe the audience to whom the data will be reported

(ii) Indicate the type of information that will be published, reported, or otherwise released

6. DATA FLOW, USE AND MANAGEMENT

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

b. Check any item(s) below that apply to the data use:

(i) ☐ Data will be accessed by login using the following access level: _____

(ii) ☐ Data will be received as an extraction provided by: _____

(iii) Equipment intended for data use is: ☐ Government Furnished Equipment (GFE)
☐ Non-Government Furnished Equipment

(iv) How often will data be obtained? ☐ Daily ☐ Monthly ☐ Yearly ☐ As needed *(explain)*

_____

7. RESEARCH REQUESTS

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

- The protocol must be approved by an Institutional Review Board (IRB)
- If the protocol was reviewed by a non-DoD primary IRB, the DHA Human Research Protections Program (HRPP) must review the research documentation
- The Sponsor must ensure that any publication/release complies with DoD requirements
- For more information, visit the *DHA Human Research Protection Program web page*
- If this request involves the use of PHI, the DHA Privacy Board will be advised. For more information about the DHA Privacy Board process, visit the *DHA Privacy Board web page*

a. Principal Investigator Information

PI Name	Research Organization

Street Address	City

State	Zip	Country

Phone Number	E-mail Address

b. Protocol Information

(i) Title of Research Project Protocol

(ii) Name of Primary IRB:

(iii) If the primary IRB is outside of the DoD, provide the DHA HRPP Protocol Review Determination reference number:

(iv) If this data use involves a survey of 10 more individuals, indicate the survey license information below:

Survey License Number: Survey License Expiration Date:

(v) If this protocol has changed, and will modify a previously executed DSA, describe the protocol changes:

8. SOURCE AND TYPE OF DATA

a. Indicate the DHA system(s) from which the data will be obtained:

- Data must be limited to the minimum necessary for accomplishing the described purpose. (*See Appendix E*)
- 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.

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

b. Identify whether the 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.

(i) ☐ This request includes specific data elements from the following system(s):

(ii) ☐ This request includes all data in the following system(s):

(iii) Provide justification for requesting the use of all data within a system:

c. Specify files and data elements. Download and attach the applicable Data Request Template (DRT).
Data specification in another format is acceptable

- DRT Military Health System Data Repository (MDR) Extractions (Enable MACROS to print only *desired variables)*
- General Data Request Template (to list extracted data from systems other than MDR)
- DRT_Access by Login (to list data intended to obtain via direct login)

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

(i) If the DHA data will be merged, linked, or otherwise associated with data from any other sources outside of DHA, explain why, and by what method the DHA and non-DHA data will be associated?

(ii) List the non-DHA systems:

9. ADDITIONAL INFORMATION

If PII will be electronically collected, maintained, used, or disseminated) provide the following information:

a. Storage database/system name:

b. System of Records Notice (SORN) number, applicable to the system in which the data will be stored, if an item, collection, or grouping of information will be created with the intent of retrieving an individual's information using a unique identifier:

10. SYSTEM SECURITY INFORMATION

If data will be stored, processed, maintained or used on DoD approved equipment, include the DoD approval information below (e.g., Authority to Operate, Interim Authority to Operate, etc.).

Consult the technical representative responsible for maintaining the computing resources proposed for this data use if necessary.

a. Provide DoD Approval Information for each system on which DHA data will be used:

List Each System or Network	Indicate Type of Approval	Expiration Date

b. List any organizations, that will store, process, maintain or use the data on equipment that is not DoD approved (e.g. contractor, academic institution equipment):

If the data contain individual identifiers, a System Security Verification (SSV) template must be completed by each organization indicated above.
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 Templates ☐ SSV Template

☐ Other (briefly describe):

Submit DSAA and supporting documentation to DSA-Mail

12. CERTIFICATIONS

The initials, provided by the Applicant and Government Sponsor, verify that the responses in this application are truthful and accurate. These representatives agree to promptly notify the Privacy Office of any project change(s) that may affect the data use reflected in this DSAA.

The parties acknowledge that after this application is approved, the Privacy Office will send the appropriate Data Sharing Agreement (DSA) to the Applicant (referenced as the Recipient on the DSA) and the Government Sponsor for signature.

After receiving the Recipient/Sponsor-signed DSA, the Privacy Office will provide final signature and forward the executed DSA, which incorporates the approved DSAA, to the Recipient and Government Sponsor.

APPLICANT	GOVERNMENT SPONSOR
By electronically initialing this application, I certify that this application is submitted with my consent	By electronically initialing this application, I certify that this application is submitted with my consent
Initials: _____ **Date:** _____	**Initials:** _____ **Date:** _____

PRIVACY NOTICE

Data Sharing Agreements are project or contract-specific, not individual data user-specific. Only the names and professional contact information of the Applicant and Government Sponsor should be listed. The names and contact information for the listed individuals are maintained so information and notices can be sent to these individuals. It may be protected under the provisions of the Privacy Act of 1974 and only released as permitted by law.

PRIVACY OFFICE SIGNATURE

DSAA APPROVAL

_____

Ms. Rita DeShields
Data Sharing Compliance Manager
Defense Health Agency Privacy and Civil Liberties Office
7700 Arlington Boulevard, Suite 5101
Falls Church, VA 22042-5101
703-681-7500

DEFENSE HEALTH AGENCY
DATA SHARING AGREEMENT APPLICATION

APPENDIX A

RESPONSIBILITIES

DSAA APPLICANT / DSA RECIPIENT RESPONSIBILITIES:

- Provide and maintain accurate and complete DSAA responses
- Agree to and execute a DSA after the DSAA is approved by the Privacy Office
- Ensure the project abides by the submitted protocol and the stipulations as stated in the DSA
- Assume physical or contractual liability for preserving the data integrity
- Fulfill Business Associate Agreement (BAA) requirements, if applicable
- Submit a DSA modification request template to notify the Privacy Office of any data use, storage or disclosure changes
- Follow DHA breach notification and response procedures (in the event of potential or actual loss, theft, or compromise of data) as outlined on the Privacy Office website
- Notify the Privacy Office, no later than 30 days after the completion of the project or the DSA expiration (unless requesting renewal), by submitting a Certification of Data Disposition (CDD)

GOVERNMENT SPONSOR RESPONSIBILITIES:

- Examine the intended project to avoid both duplication and unnecessary generation of DHA data
- Verify that the data are used in compliance with applicable privacy and security standards
- Confirm that publications, or any other release of data results/findings, adheres to DoD requirements
- Affirm scientific merit, feasibility and usefulness in relation to the MHS mission, goals, and objectives
- Assure that the project outcomes will benefit DoD
- Certify that accurate and complete responses are reflected in the DSAA
- Agree to and execute a DSA once the DSAA is approved by the Privacy Office
- Provide Applicant/Recipient oversight for the duration of the project reflected in the DSA
- Ensure that the BAA requirements, if applicable, are fulfilled
- Assure that DHA 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
- Serve as the Government (military or DHA civilian personnel) Point of Contact
- Maintain current contact information with the Privacy Office
- Sign a DSA modification request template to endorse any data use, storage or disclosure changes
- Endorse timely DSA renewal, if necessary
- Authorize the submission of a CDD no later than 30 days after DSA expiration

DEFENSE HEALTH AGENCY
DATA SHARING AGREEMENT APPLICATION

APPENDIX B

DE-IDENTIFIED, AGGREGATE, SENSITIVE AND PROPRIETARY DATA

A. The HIPAA Privacy Rule provides two methods by which health information may be de-identified
   1. Expert Determination Method:
      - This expert must have knowledge of and experience with the statistical and scientific procedures used to de-identify PHI and is competent in determining that the risk of identifying an individual from the de-identified data, when used alone or in combination with other information, is very small.
      - This expert must document the methods and results of the analysis that justify such determination.
   2. Safe Harbor Method:
      - All 18 of the HIPAA direct individual identifier categories (including those of the individual or their relatives, employers, or household members) are removed.

B. Data Aggregation is included in the Final Rule's list of business associate services
   1. Data aggregation involves grouping independent but similar information components of gathered data into summary form, generally for purposes such as statistical analysis (i.e., grouping summary information about specific groups based on definite variables such as age, profession, or income).
   2. Aggregate data is not automatically categorized as de-identified data. To ensure that aggregated health data is de-identified in compliance with HIPAA, the appropriate methods must be used to determine that the data cannot be used alone or in combination with other information to identify an individual.

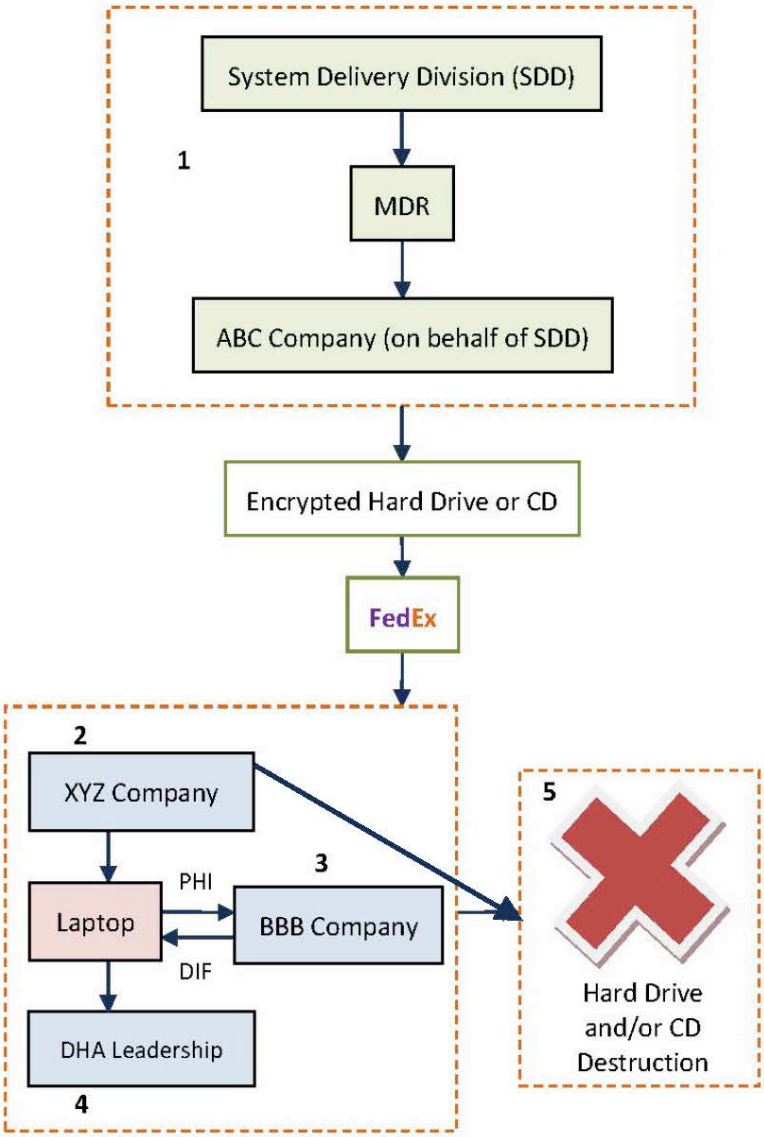
C. The potential use of or access to sensitive or proprietary business, technical, financial, and/or source selection information belonging to the Government or other contractors must be safeguarded so as not to cause adverse effects on organizational operations, organizational assets, or individuals.
   1. Protection of proprietary information prevents the compromise of property rights or economic interest, reduces risk to a contractor's commercial position, and safeguards the Government's ability to obtain access to or use of the data.
   2. Sensitive data includes cost comparisons and price quotes, Government spend plan data, contractor technical proposal data, independent Government cost estimates, negotiation strategies and contractor data presented in negotiations, contracting plans and statements of work.

D. When documenting the intended method of de-identification, keep the following questions in mind:
   1. How will the 18 categories of HIPAA identifiers be removed? (explain encryption/redaction processes)
   2. How will small cell size be determined?
   3. How will small cell sizes be eliminated? (i.e., redacted, rolled up, etc.)
   4. How will the process for ensuring minimum risk of data re-identification be explained?
   5. How will the combination of fields be reduced to ensure minimum risk of re-identification?
      (In other words, how will the requestor deal with the potential ability to triangulate data to come up with data that's small enough to identify an individual?)
      - Examples of combination fields:
        i. Cross tab of data sets
        ii. Connecting data (i.e., users with access to areas where data may be combined with information obtained from another system, potentially deducing a person's identity)

DEFENSE HEALTH AGENCY
DATA SHARING AGREEMENT APPLICATION

APPENDIX C

EXAMPLE DATA FLOW (AS INDICATED IN SECTION 5A)
Data Flow Diagram – XYZ Company for DSAA #XX-XXXX "Analysis for DHA Leadership"



Data Flow:

1. ABC Company (on behalf of SDD) will extract PHI from the MDR and send to the DSA Recipient (XYZ Company) via encrypted (using Guardian Edge) CD or hard drive via FedEx.
2. Once received, XYZ Company will load the data onto one (1) laptop. Access to the data will be limited to XYZ Company analysts and BBB subcontractors with need to know.
3. Subcontractor BBB will access the PHI on the XYZ Company laptop for the sole purpose of de-identifying the data as per HIPAA guidelines. Identifiers will be deleted or encrypted.
4. DHA leadership will receive a copy of the summarized results only.
5. Upon completion of the project, the original CD on which the data was received will be destroyed by a shredder. XYZ Company will delete the data from the laptop and perform a wipe of the laptop hard drive.

DEFENSE HEALTH AGENCY
DATA SHARING AGREEMENT APPLICATION

APPENDIX D

HIPAA DEFINED BUSINESS ASSOCIATE FUNCTIONS AND SERVICES

A. An individual or organization, that performs one or more of the following functions or services on behalf of a covered entity, may be a business associate, according to HIPAA:

1. Performs or assists in performance of one or more of the following functions or activities, involving the use or disclosure protected health information (PHI), such as:
   - Data analysis
   - Claims processing or administration
   - Utilization review
   - Quality assurance reviews
   - Any other function or activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule
2. Performs one or more of the following services to or for a covered entity, involving the use or disclosure of PHI, such as:
   - Legal
   - Actuarial
   - Accounting
   - Consulting
   - Data aggregation
   - Management
   - Administrative
   - Accreditation
   - Financial
3. Provides data transmission services of PHI to a covered entity (e.g., Health Information Organization, E-prescribing gateway)
4. Accesses PHI to provide a personal health record on behalf of a covered entity
5. Works for a business associate that delegated a function or service to you that the business associate agreed to provide for a covered entity or for another business associate

B. An individual or organization that fits into one of the four exceptions listed below may not meet the definition of business associate:

1. Covered entity in an organized health care arrangement, performing a covered function/service to, for, or on behalf of the arrangement
2. Government agency that receives or collects PHI to determine eligibility or enrollment in a Government health plan
3. Plan sponsors who only receive PHI from a group health plan that meets HIPAA requirements
4. Health care providers who only receive PHI from a covered entity for purposes of treating individuals

DEFENSE HEALTH AGENCY
DATA SHARING AGREEMENT APPLICATION

APPENDIX E

A. DEFINITIONS

Business Associate: A person or entity, who is not a member of the covered entity's workforce, that creates, receives, maintains, or transmits PHI on behalf of the covered entity or in providing a HIPAA-allowed service to the covered entity that involves the use or disclosure of PHI.

Covered Entity: A health plan, a health care clearinghouse, or a health care provider that conducts one or more HIPAA-covered transactions in electronic form.

DSA Recipient: The individual who initials the DSAA as "Applicant," and functions in the role of Recipient upon DSA execution.

DSAA Applicant: The individual who completes and submits a DSAA and serves as the primary point of contact during the Privacy Office approval process. This individual is generally employed by a non-DoD organization (i.e., contractor, grant recipient, research staff) that supports a Government project or research. Government personnel may meet the definition of Applicant if the data use involves only Government staff (no contractor participation).

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 HIPAA.

Minimum Necessary: A covered entity must make reasonable efforts to limit the use, disclosure, or request of PHI to the minimum necessary for accomplishing the described purpose. HIPAA's minimum necessary rule does not apply when disclosing PHI for treatment, to a medical training program, when disclosed to the individual, pursuant to an authorization.

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 DHA in its role as an employer.

B. FEDERAL LAW

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

HIPAA Privacy and Security Rules (45 C.F.R. 160 & 164)

C. 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, Dec. 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