

## PRIVACY IMPACT ASSESSMENT (PIA)

**PRESCRIBING AUTHORITY:** DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

**1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**

Electronic Institutional Review Board (EIRB)

**2. DOD COMPONENT NAME:**

Defense Health Agency

**3. PIA APPROVAL DATE:**

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** (Check one. Note: foreign nationals are included in general public.)

- |  |  |
|--|--|
| <input type="checkbox"/> From members of the general public  | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)   |

**b. The PII is in a:** (Check one)

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> Significantly Modified DoD Information System |   |

**c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.**

The mission of the research protection program is to foster and oversee research and development activities by promoting policies and procedures that facilitate timely and effective reviews of research and ensuring that approved research is conducted in accordance with applicable federal codes and ethical guidelines to protect the rights and welfare of human research participants, including service members, employees, and their families. The purpose of EIRB is to track research protocols from inception throughout the entire life cycle of the project to ensure compliance as well as ensuring the individuals engaged in the performance of research at Department of Defense (DoD) institutions are properly trained and qualified.

The EIRB is a world-wide, 24/7 accessible, Common Access Card (CAC), External Certificate Authority (ECA) and Veteran Affairs Personal Identity Verification (PIV) authentication, web-based business platform that allows horizontal and vertical multi-level transparency to foster collaboration, submission, management, tracking, oversight, auditing, and reporting of clinical and graduate medical education research and related projects throughout their life cycle.

Types of personally identifiable information (PII) that may be collected include personal descriptors, contact information, gender, and education background. Information will be collected from any category of individuals that use this system to submit a research proposal and/or review the proposal. PII is only collected from the EIRB end users. EIRB end users are Research and Review Board staff. Researchers can include Principal Investigators, Co-Investigators, Associated Investigators, Research Coordinators, Participating Clinicians and Statisticians. Reviewers can include Review Board Members, Chairpersons, Board Coordinators and Institutional Review Board Managers.

EIRB is owned and managed by the Clinical Support Program Management Office (PMO), Solution Delivery Division, J-6, Defense Health Agency (DHA).

**d. Why is the PII collected and/or what is the intended use of the PII?** (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)

The PII collected will be used for identification, tracking, and oversight of researchers to ensure that everyone engaged in the performance of research at the DoD member institutions are properly trained and qualified. The mission of the research protection program is to foster and oversee research and development activities by promoting policies and procedures that facilitate timely and effective reviews of research and ensuring that approved research is conducted in accordance with applicable rules and ethical guidelines to protect the rights and welfare of the participants, including service members, employees, and their families.

**e. Do individuals have the opportunity to object to the collection of their PII?**  Yes  No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals can object by not submitting requests for approval to engage in or to conduct research. The submission of PII in the system is voluntary. However, failure to provide the PII will result in the individual not being able to conduct research at any of the member DoD institutions.

f. Do individuals have the opportunity to consent to the specific uses of their PII?  Yes  No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

PII is collected in the system to permit identification, tracking, and oversight of authorized research procedures and to track the individual researchers and reviewers involved in the process. The purpose of tracking individuals is to ensure that everyone engaged in the performance or oversight of research is properly trained and qualified. For research audit purposes, identification of the individual making determinations about the research proposal is necessary.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)

Privacy Act Statement  Privacy Advisory  Not Applicable

AUTHORITY: 32 CFR 219, Protection of Human Subjects; DoD Instruction 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD Supported Research; and DoD Instruction 3216.01, Use of Animals in DoD Programs.

PURPOSE: Information collected from you will be used for identification, tracking and oversight of researchers to ensure that everyone engaged in the performance of research at the DoD member institutions are properly trained and qualified.

ROUTINE USES: Information in your records may be disclosed to Federal, State, local, or foreign government agencies for identification, tracking and oversight of authorized research procedures and tracking of individual researchers and reviewers involved in the process.

For a full listing of applicable Routine Uses, refer to the applicable SORN

APPLICABLE SORN: EDHA18, Research Regulatory Oversight Records is the System of Records Notice (SORN) applicable to this information system. The SORN can be found at: <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570681/edha-18/>

DISCLOSURE: Although providing information is voluntary, in that you will not be subject to any criminal penalties for not providing the information, failure to do so may result in individual not being able to conduct research at any of the member DoD institutions.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)

- Within the DoD Component Specify. 

DHA/HA institutions: Acquisition, Technology, and Logistics (AT&L), Personnel and Readiness (P&R)
Army, Navy, Air Force, Acquisition, Technology, Personnel and Readiness (P&R)
According to DoD Instructions 3216.01 and 3216.02, the Under Secretary of Defense for Personnel and Readiness has delegated responsibilities with respect to matters affecting medical research to the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). Therefore, the system is centrally managed and owned by DHA, Clinical Support PMO, but is available to all Service Medical Components. EIRB is permitted to retrieve information about each individual whose information is collected into EIRB as that individual engages in research, conducts research, or reviews, approves, or oversees such research.
- Other DoD Components Specify. 

--
- Other Federal Agencies Specify. 

--
- State and Local Agencies Specify. 

--

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)

Aderas, Inc provides Tier III application support to the EIRB DoD research protection program.

Specify.

No contractor maintains PII at a contractor location. All contractor access to EIRB is via the DISA Out-of-Band (OOB) Virtual Private Network (VPN) which is encrypted using Federal Information Processing Standards (FIPS) 140-2 compliant encryption algorithms.

All contracts contain language which require the contractor to comply with the Privacy Act of 1974, as amended.

Other (e.g., commercial providers, colleges).

Specify.

**i. Source of the PII collected is:** (Check all that apply and list all information systems if applicable)

Individuals

Databases

Existing DoD Information Systems

Commercial Systems

Other Federal Information Systems

While using the EIRB application request page, the DHA Identity Authentication Services (iAS) system provides EIRB with the user's first name, last name, DoD certificate number, and certificate email address.

**j. How will the information be collected?** (Check all that apply and list all Official Form Numbers if applicable)

E-mail

Official Form (Enter Form Number(s) in the box below)

Face-to-Face Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

EIRB Website Uniform Resource Locator (URL): <https://eirb.csd.disa.mil>

Individuals accessing the system must have a DoD CAC, PIV, or ECA and request an account through the EIRB account request page or via submission of a DHA Global Service Desk ticket. The EIRB system does not use user name or password to access the system.

The initial collection of data includes first name, last name, DoD certificate number, and certificate email address. Any additional account information is filled out by the user after logging into the EIRB system. The EIRB help desk may need to contact the user via telephone or email to obtain this information. The EIRB system populates any changes or updates to account information during the authentication process using the DHA iAS system.

**k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

Yes  No

If "Yes," enter SORN System Identifier

EDHA 18

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.defense.gov/Privacy/SORNs/>  
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

**l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

(1) NARA Job Number or General Records Schedule Authority.

N1-330-08-8

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Retention: Delete/destroy 10 years after completion or termination of the research protocol (coincides with the term of the research).

**m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.**

- (1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
- (2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).
  - (a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.
  - (b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.
  - (c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

32 CFR 219, Protection of Human Subjects; DoD Instruction 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD Supported Research; and DoD Instruction 3216.01, Use of Animals in DoD Programs.

**n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes     No     Pending

- (1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
- (2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
- (3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

0720-0042, Expiration: 07/31/2020