PRIVACY IMPACT ASSESSMENT (PIA)

For the

Blood Donor Management System (BDMS)
Defense Heatlh Agency (DHA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number: 13520 (EBMS)

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI UII = 007-000003993 (EBMS)

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier EDHA 07

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	BDMS is in process of receiving an OMB Control Number.
Enter Expiration Date	

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

10 U.S.C., Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of the Blood Donor Management System (BDMS) is to manage the blood donation aspect of the Armed Services Blood Program (ASBP), including blood donor registration, screening, blood products, and associated record keeping for military blood donors, dependents of military donors, and other civilian donors in the Continental United States (CONUS), Outside Continental United States (OCONUS), and in Theater.

BDMS is part of the Enterprise Blood Management System (EBMS) products initiative which will employ two separate and distinct FDA regulated Class II Medical Devices – BDMS and the Blood Management Blood Bank Transfusion Services (BMBB/TS) – providing an effective "arm-to-arm" solution. BMBB/TS will manage the blood transfusions process.

BDMS and BMBB/TS will replace the current legacy system, the Defense Blood Standard System (DBSS).

BDMS will be accessible by authorized users (i.e., government civilians, military government contractors, and other contract support) from 24 Military Treatment Facilities (MTFs). The system hosts a web application that will not be accessible by the public; rather, it will be restricted to authorized users.

The types of personal information collected in BDMS includes personal descriptors, ID numbers, ethnicity, health, employment, and life information.

This system is owned and managed by Defense Health Clinical Systems (DHCS), which is a Military Health System (MHS) / Defense Health Agency (DHA) Program Office. The Commercial off the Shelf (COTS) medical device manufacturer is Mediware Information Systems, Inc.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

All applicable security and privacy processes and regulations (e.g., the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Privacy Act of 1974, as amended, etc.) have been defined and implemented, reducing privacy risks to the maximum extent possible.

The DISA computing facilities housing the BDMS application and network communication servers have comprehensive physical, technical, and administrative controls, in accordance with Department of Defense (DoD) 8580.02-R, DoD Health Information Security Regulation for MAC II Sensitive systems. Office door locks, password-enabled screen savers, monitoring by facility staff, application time-outs, and BDMS technical controls that prevent unauthorized individuals from logging onto the system provide protection for PII stored in BDMS.

The system architecture security requirement ensures that the system security safeguards are protected from access, modification, and destruction by unauthorized personnel.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. MTF Occupational Health Departments (in order to disclose to military personnel a positive test result)

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Planned Systems International (PSI), Inc.
10632 Little Patuxent Parkway, Suite 200
Columbia MD, 21044

Mediware Information Systems, Inc.
11711 West 79th St.
Lenexa, KS 66214

The following language is contained in all contracts and sub-contracts awarded by the government:

"The DHA Privacy Office website at http://www.tricare.mil/tmaprivacy/contract.cfm contains guidance regarding Protected Health Information (PHI) and Personally Identifiable Information PII). The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data.

The Contractor shall ensure that data which contains PHI is continuously protected from unauthorized access, use, modification, or disclosure. Contractor shall comply with all previously stated requirements for HIPAA, Personnel Security, Electronic Security, and Physical Security."

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

Specify. Local Disease Control (in order to disclose to a civilian a positive test result)

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

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

Blood donations are a voluntary process. If an individual objects to the collection of their PII / PHI at the time of a blood drive / blood donation, the individual is not obligated to give blood; however, individuals will not be able to donate blood unless PII / PHI is provided.

(2) If "No," state the reason why individuals cannot object.

j. 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.

ASBP has published a manual (TM 8-227-11) for the collection of blood. Per TM 8-227-11, the donor must complete Uniform Donor Health Questionnaire (UDHQ) form, or equivalent.

The UDHQ requests information of the individual and explains the use of the individual's PII and includes a Privacy Act Statement and Statement of Consent. When an individual sign the forms, he or she gives their consent to use their PII.

Consent to the specific uses of PII is obtained as necessary in accordance with DoD 5400.11-R, Department of Defense Privacy Program, C.4.1.3.

PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to authorize or restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R.

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

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.

The Privacy Act Statement and Statement of Consent are located on the reverse side of Uniform Donor Health Questionnaire (UDHQ).

This statement serves to inform you of the purpose for collecting your personal information and how it will be used.

AUTHORITY: 10 U.S.C., Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities; and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from you in order to determine suitability of voluntary blood donations, record time of withdrawal and blood type, administer the Armed Services Blood Program, and in some cases to recommend medical treatment.

ROUTINE USES: Information in your records may be disclosed to the Departments of Veterans Affairs and Health and Human Services in connection with medical care matters and collaborative research activities. Information may also be provided to other federal, state, and local government units for compliance with laws governing blood supply safety, control of communicable diseases, preventive medicine and safety, and public health mandates relating to blood supplies.

Your records may be disclosed outside of DoD in accordance with the DoD Blanket Route Uses published at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and discloses of PHI include, but are not limited to, treatment, payment, and healthcare operations.

DISCLOSURE: Voluntary. However, failure to provide complete information will make you ineligible to donate blood at this time.

STATEMENT OF CONSENT: It has been explained to me that blood donation is a voluntary process requiring the collection of approximately 450-500 mL of blood. The collection time usually ranges from 5 to 10 minutes. Complications at the venipuncture site may include, but are not limited to: discomfort, bruising, swelling, or infection. Other complications could include: fatigue, light-headedness, dizziness, nausea, vomiting, and/or fainting. On very rare occasions, a more severe reaction may occur. I have reviewed and understand the information provided to me regarding the spread of the AIDS virus (HIV) by blood and plasma. If I am potentially at risk for spreading the virus known to cause AIDS, I agree not to donate any blood products for transfusion to another person or for further manufacture. I understand that my blood will be tested for antibodies to HIV, Hepatitis B, Hepatitis C, and other disease markers. If this testing indicates that I should no longer donate blood or plasma because of a risk of transmitting these viruses, my name will be entered on a list of permanently deferred donors. I understand that I will be notified of positive results. For active duty personnel, reservists, and accessions, I understand positive screening and confirmatory results will be forwarded to appropriate medical personnel for further evaluation, and if required “fitness for duty” determination. If instead, the result of the testing is not clearly negative or positive, my blood will not be used and my name may be placed on a deferral list without my being informed until the results are further clarified. I understand there are rare circumstances, due to blood tubes not being collected or due to specimen acceptability, in which infectious disease testing may not be performed on my blood. I understand that if a computer assisted interview is completed, only the questions I have answered that require further information will be printed on this form. I understand there is a separate statement of consent containing additional information related to Apheresis donations. I have been given an opportunity to ask questions and have had a chance to refuse the phlebotomy procedure. My signature below indicates my consent to have a phlebotomist collect blood from me today.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.