PRIVACY IMPACT ASSESSMENT (PIA)

For the

Center for Disease Detection Laboratory Information System (CDDLIS)
US Army Medical Command - DHP Funded System

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

☐ **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

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

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.

5 U.S.C. 301, Department Regulation; 10 U.S.C., Chapter 55; Pub.L. 104-91, Health Insurance Portability and Accountability Act of 1996; DoD 6025.18-R, DoD Health Information Privacy Regulation; 10 U.S.C. 1071-1085, Medical and Dental Care; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b, TRICARE Prime and TRICARE Program; 10 U.S. C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD 6010.8-R, CHAMPUS; 10 U.S.C. 1095, Collection from Third Party Payers Act; and E.O. 9397 (SSN).

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 Center for Disease Detection has developed the Laboratory Information System to securely process and report results of blood samples of DoD military personnel. The system uses standard server, workstation, and networking components. Commercial off the Shelf (COTS) products are configured and integrated in accordance with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) to provide secure system access, data processing, and data protection. The CDDLIS disease detection process incorporates the collection and processing of blood samples; automated and manual order processing; authenticated user access to obtain lab test results; and logistics support. The CDDLIS is capable of securely processing blood samples and reporting test results within 12 hours of receipt of sample.

Personal information collected includes name, date of birth, gender, Social Security Number, and medical information.

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

The privacy risks associated with the PII collected are unauthorized access and unauthorized disclosure. There are security measures in place to mitigate these risks. These security measures are addressed in item 3d and 3f below.

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. Army military treatment facilities (MTFs) that submit samples for testing.

☒ **Other DoD Components.**

Specify. Navy
US Military Entrance Processing Command (MEPCOM)
Army National Guard
Armed Forces Health Surveillance Center (AFHSC).

☒ **Other Federal Agencies.**

Specify. US Coast Guard

☐ **State and Local Agencies.**

Specify.

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

Specify.

Center For Disease Detection, LLC.
11603 Crosswinds Way, Ste 100
San Antonio, TX 78233

11.5. SECURITY REQUIREMENTS: The Contractor shall be responsible for the security of all patient information, testing results, specimens, supplies, materials, and equipment and will ensure compliance with all applicable security requirements of HIPAA, DoD regulations/guidance (including but not limited to Military Health System Automated Information Security; Privacy Act and data at rest policies), and this PWS. (See ATTACHMENT 3 – Privacy Act and Security Clearance and ATTACHMENT 4 – MHS Interface Requirements).

2.1.131 The Contractor will ensure the protection of all sensitive, private, protected, and patient/applicant/source health information. Additionally, neither the Contractor nor any of the contract service providers shall disclose or cause to disseminate any information concerning operations of military activities. Such action(s) could result in violation of the contract and possible legal actions. If there is a loss or compromise of any protected data, the Contractor will indemnify the Government and ensure that the Government bears no cost.

2.1.135 Security. The Contractor shall meet all DoD and National Security Agency guidelines for automated data processing, computer security, personnel security, validation, and audit requirements.

1.5.5.3. HIPAA requirements of electronic transmission of individually identifiable patient information.

1.5.6.3. Data Security. The Contractor shall provide a mechanism for maintaining and protecting data integrity from intrusion, contamination, or unauthorized modification. The Contractor shall maintain surveillance protocols and procedures and will (1) notify the KO within one hour of any unauthorized, real or probable system breach: (2) take immediate measures to (a) remove system weakness(es) that led to breach; (b) determine impact; and (c) inform KO of extent of damage and efforts to correct data and prevent recurrence. Full occurrence report will be provided within 10 business days. Contractor will also provide a monthly report of any attempts to invade the system.

1.5.6.4. Secure electronic data transfer between the Contractor and designated Government locations.

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

Specify.

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.

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

The individuals do not participate in the PII collection process for this system. PII is collected from existing DoD systems - Composite Health Care System (CHCS) and Navy Human Immunodeficiency Virus Management System (HMS).

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.

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

The individuals do not participate in the PII collection process for this system. PII is collected from existing DoD systems - CHCS and Navy HMS.

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 individuals do not participate in the PII collection process for this system. PII is collected from existing DoD systems - CHCS and Navy HMS.

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.