PRIVACY IMPACT ASSESSMENT (PIA)

For the

Nutrition Management Information System (NMIS)
Defense Health 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: 161
- ☐ **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: 007-000000106

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 17

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.

10 U.S.C. Chapter 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1338.10, Department of Defense Food Service Program; 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 this system is to facilitate the Medical Nutrition Therapy (MNT) Health Care Program and to control health care costs. The MNT will enable the provider to track a patient's progress in relation to the nutrition care outcomes associated with the diagnosis. The program provides an effective and efficient method of preventing inpatient episodes, lowering morbidity, and progressing towards optimal health.

NMIS is a Tri-Service automated information system (AIS) to support the nutritional management functional area. The nutrition community will utilize this commercial off the shelf (COTS) system to replace the legacy NMIS. NMIS supports the mission of providing preventive and therapeutic MNT and Medical Food Management (MFM). NMIS supports standard operating procedures (SOPs) based on DoD policies as well as standards imposed by the American Dietetic Association (ADA), Joint Commission on the Accreditation of Health Organizations (JCAHO), and Occupational Safety and Health Administration (OSHA).

NMIS has four components: Foodservice Operations Management (FOM), Nutrition Care Management (NCM), Room Service (RS), and Pending Diet Orders (PDO).

- The FOM module provides menu planning, purchasing, inventory, production, recipe management, forecasting, food and labor costing, and nutrient labeling capabilities.

- The NCM module provides the ability to track patient, resident, or client demographics, acuity levels, diet orders, weight history, as well as any likes, dislikes, or allergies. NCM also provides menu and tray ticket production, nutrient analysis, recipe, and menu management.

- The RS module is a restaurant menu-style feeding function which allows individuals to select and order meals through either bedside entry and/or telephone ordering system via a call center. This information goes from a patient to a diet technician into NMIS.

- The PDO solution is an add-on module to the Hospitality Suite’s Diet Order interface. With the add-on module, Nutrition Services has the advantage of inputting PDO data in advance and having the system automatically transfer the information in the patient’s diet order, categorizing the order in, next, or past meal status.

NMIS collects the following types of personal information about individuals:
Name
Social Security Number (SSN) (or other unique identifier)
Medical Record Number (Family Member Prefix (FMP))
Race/Ethnicity
Birth Date
Title/Rank
Religious Preference
Medical Information (Allergies, Diagnosis, Height, Weight, Diet Orders and Ward/Room/Bed Assignments)

PII/PHI is collected from Members of the Armed Forces, their family members, and other individuals entitled to DoD health care that receive nutrition care intervention at one or more of the DoD's MTFs.

The system point of contact is:
NMIS Project Officer
DHHQ
7700 Arlington Blvd
Falls Church, VA 22042

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

Any perceived privacy risks regarding the collection, use and sharing of PII/PHI in the system have been minimized through system design and implementation of various administrative, technical, and physical security controls.

Access to personal information is limited to those who require the records to perform their official duties. All personnel whose official duties require access to the information are trained in the proper safeguarding and use of the information. NMIS confidentiality is ensured through both technical and administrative means. Technical means provide the ability to employ role separation and auditing down to the field level to ensure that information cannot be disclosed without proper permissions. Administratively, personnel are subject to appropriate background investigations before being given access to the system and must undergo security awareness training to ensure that DoD 5400.11-R, "Department of Defense Privacy Program" policies are understood.

Additionally, access to the NMIS application requires authorization to login to the MHS network. MHS account group policies prevent unauthorized access to NMIS. NMIS is classified as a MAC III sensitive system and users must complete mandatory IA Awareness Training and HIPAA training prior to accessing and to maintain their access to the system. Further, a Common Access Card (CAC) is required for use of the system including a 2-factor authentication and pin created by the user.

Documented procedures are in place to identify and respond to security breaches or disclosures of personal information. In case of any such breaches or disclosures, the DHSS Program Office will be notified immediately to resolve the situation. Protecting the privacy and security of personally identifiable information (PII) and protected health information (PHI) is the responsibility of all Defense Health Agency (DHA) and MHS workforce members, to include the organization's civilian employees, uniformed service members, and contractors requiring access to PII and PHI. Personnel will follow the reporting and notification requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; and DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.

The end user will view the DoD warning banner and the Privacy Act warning when
logging in to the system. The DoD banner for NMIS is stated as follows:

You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only. By using this IS, (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications occurring on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using or data stored on this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Information contained in this system is subject to the Privacy Act of 1974 (5 U.S.C.552A, as amended). Personal information contained in this system may be used only by authorized persons in the conduct of official business. Any individual responsible for unauthorized disclosure or misuse of personal information may be subject to a fine of up to $5,000.

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. CliniComp's Essentris Clinical Information System–Intelligent Charting and Surveillance Electronic Health Record (EHR) (this system was formerly known as CIS).

☐ **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.

☐ **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.

Submission of information is voluntary. However, if an individual refuses to provide needed information, comprehensive health care may not be possible.

(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.

PII/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 restrict the use of their PII/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, C10.1.

(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.

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

AUTHORITY: 10 U.S.C. Chapter 136, Under Secretary of Defense for Personnel and Readiness; DoD Instruction 1338.10, Department of Defense Food Service Program; and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information necessary to carry out the Medical Nutrition Therapy (MNT) Health Care Program and to control health care costs.

ROUTINE USES: Use and disclosure of your records outside of DoD may occur in accordance with the DoD Blanket Route Uses published at http://dpclo.defense.gov/privacy/SORNs/blanket_routine_uses.html 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: Submission of information is voluntary. However, if an individual refuses to provide needed information, health care outcomes may be less than optimal.

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.