



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Nutrition Management Information System (NMIS)
--

TRICARE Management Activity (TMA)
-----------------------------------

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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**

MHS beneficiaries

**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.

7 U.S.C. Chapter 84 (National Nutrition Monitoring and Related Research); 45 C.F.R. Part 160 and Subparts A and E of Part 164 (HIPAA Privacy Rule); DoDI 1338.10 (Manual for the Department of Defense Food Service Program); 72 FR 5019 (DHA 17 - Nutrition Management Information System, February 2, 2007); and E.O. 9397 (as amended, November 20, 2008, for SSN collection).

**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 three components: MNT, MFM and Room Service (RS).

MNT provides an effective and efficient method of preventing inpatient episodes, lowering morbidity, and progressing towards optimal health outcomes. The goals of MNT are to achieve a healthier population, slow disease progression (disease management), and standardize clinical practice patterns. MNT is a tool that supports data collection and analysis of nutrition intervention clinical outcomes.

MFM supports quantity food production management and the service aspects of fulfilling patient diet orders. Activities include procuring commodities as well as preparing, distributing, and serving meals to patients, medical treatment facility (MTF) staff and their guests.

The RS module is a bedside, restaurant menu-style feeding system which provides on-demand meals through telephone orders from a patient to a diet technician.

Personally identifiable information (PII)/protected health information (PHI) collected in this system includes name, rank, title, family member prefix, social security number (SSN), religion, allergies, date of birth, 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.

System point of contact:  
NMIS Project Officer  
5205 Leesburg Pike  
Skyline One, Suite 1000  
Falls Church, VA 22041  
Telephone number: (703) 681-3901

(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.

**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.

**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.	In addition to the Privacy Act Statement (PAS) the patient is provided with a copy of The MHS Notice each of Privacy Practices (NOPP) which includes use of PII/PHI for health care operation.  The end user will view the DoD warning banner, HIPAA banner and the Privacy Act warning when logging in to the system.
----------------------------------	--