



PRIVACY IMPACT ASSESSMENT (PIA)

For the

MAXIMUS Federal Services National Quality Monitoring Contractor (NQMC) MAXQA System
--

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

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.

32 CFR 199.15 (TRICARE's Quality and Utilization Review Peer Review Organization Program); 36 CFR 1222.48 (Data created or received and maintained for the Government by contractors); Department of Defense Administrative Instruction Number 15; TRICARE Operations Manual 6010.51-M, August 2002, Chapter 2, Section 1 (Records Management (General)).

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 MAXIMUS Federal Services NQMC system has been designed to support the Military Health System (MHS)/TMA in ensuring that quality healthcare is being provided to the beneficiaries of MHS. Data provided by TMA is reviewed by MAXIMUS NQMC according to various TRICARE contracts to ensure the quality of care being provided. The MAXIMUS NQMC MAXQA data system holds selected TRICARE Encounter Data (TED) claims record field information related to care provided in the Purchased Care System. Each month TMA provides another 1,475 claims records (files) to MAXIMUS and these files are stored in a SAS server. The primary responsibilities of NQMC includes:

- ~Retrospective Chart Review for Quality of Care
- ~External Reviews for TMA Appeals, Hearings, and Claims Collection Division
- ~Medical Necessity (Reconsideration) Appeals
- ~Military Treatment Facility Standard of Care Peer Reviews
- ~Mental Health Facility Certifications
- ~Focused Studies
- ~Technology Assessments

The data fields include name, gender, social security number (SSN), date of birth (DOB), health care diagnoses, procedures performed, dates of service, and location of care, in addition to other non-identifying information. The SAS server connects to an ORACLE database, in which some of the same PII is contained. The SAS and ORACLE databases compose the MAXQA Information System and are housed in Reston, VA. The MAXQA Information System can be accessed in Reston, VA where the servers are caged and in Phoenix, AZ where the work stations are. Information flows between the two sites through an AT&T frame relay. The only outflow of data is through a secure connection to the TMA E-Commerce Extranet to upload routine reports. A Web site exists for the NQMC Project, however, that is not hosted by the MAXIMUS NQMC Information System. The Web site for the NQMC Project is part of the MAXIMUS, Inc. corporate Web site. No protected health information (PHI), personally identifiable information (PII), or sensitive information (SI) is contained on the NQMC Project web site. There is no ability to connect to the Web site from the MAXQA Information System or to connect from the Web site to the MAXQA Information System. The MAXIMUS NQMC Information System is classified as Mission Assurance Category III Sensitive.

Program Name: TMA National Quality Monitoring Contractor
POC Title: NQMC Project Manager
Address: 1600 East Northern Avenue, Suite 155, Phoenix, AZ 85020
Main Telephone Number: 602-308-7160

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

There are no unique risks to the MAXIMUS NQMC MAXQA Information System. The risks that do exist are common to all Information Systems and include the risk of intrusions including from crackers/hackers; malicious computer code including viruses and worms; unauthorized access or unauthorized utilization of resources; disruption of services; espionage; hoaxes; and technical vulnerabilities inherent within the hardware and software.

MAXIMUS NQMC has redundant mitigations against the risks, which fall into three general categories: Information Technology, Personnel, and Physical. The MAXQA Information System bidirectionally passes information from Reston, VA to Phoenix, AZ through an AT&T frame relay. The MAXQA Information System has only one work station that has access to the Internet and that is through switches, routers, and a firewall located in Reston, VA that allows a Secure Socket Layer IP address to IP address connection to the TMA E-Commerce Extranet System (DOCUMENTUM). The PII/protected health information (PHI) is safeguarded within DoD Information Assurance Certification & Accreditation Process (DIACAP) approved policies and procedures that control information technology (IT), physical, and personnel security. Physical and IT security starts with the rare and controlled Internet access that only allows a virtual private network (VPN) connection to the TMA E-Commerce Intranet system.

Physical security include limited access to servers and PCs, photo ID key card entry under closed circuit camera, visual challenge at entry, monitor screens not visible from outside, and secure walls and ceilings. Personnel security starts at hire, includes training, routine training, and monitoring. Other IT security includes passwords, timeouts, administrative controls, routine training, monitoring, Basic Input/Output System (BIOS) two-person controlled portable e-media access, and requirement for encrypted portable e-media.

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.

There is no data exchange. Routine reports are provided as Microsoft Office documents to TMA. The reports are encrypted and sent through a Secure Socket Layer IP address to IP address. The connection is only opened for the uploading of reports into the TMA E-Commerce Extranet site. One report a month contains some first and last names and Unique Claim Numbers assigned by TMA along with a brief description of the care provided that was not a TRICARE benefit, was coded incorrectly, was not preauthorized, or was not appropriate.

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.

PII/PHI is collected so that NQMC can conduct peer reviews of healthcare provided to TRICARE beneficiaries. Quality assessment and improvement activities fall within the definition of healthcare operations under DoD 6025.18-R, DoD Health Information Privacy Regulation. That regulation permits TRICARE, as covered entity under the Health Information Portability and Accountability Act (HIPAA), to use or disclose PHI for its own healthcare operations. Individuals are not entitled to object to information collection for such a permitted use or disclosure of PHI.

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.

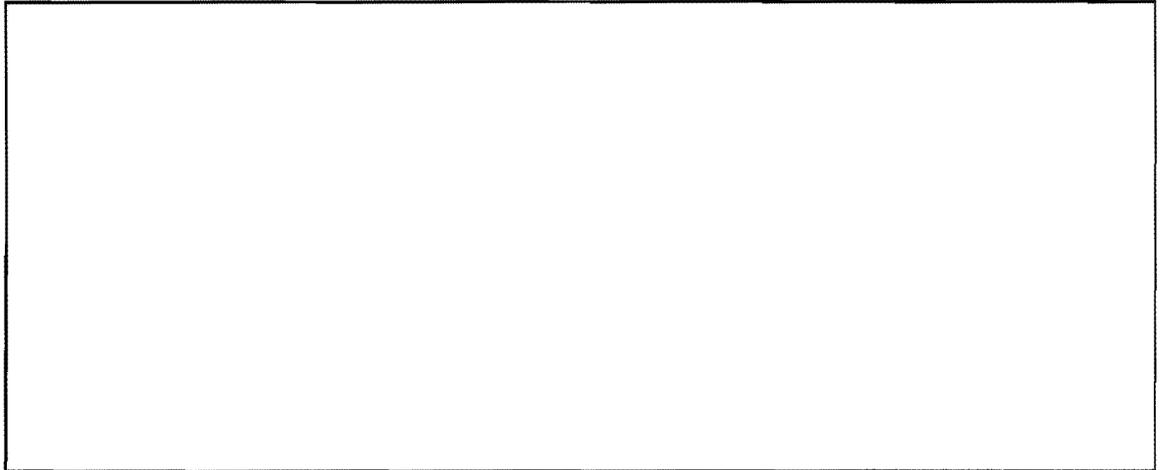
PII/PHI is collected so that the NQMC can conduct peer reviews of healthcare provided to TRICARE beneficiaries. Giving individuals the opportunity to withhold their consent to use of their PII/PHI would interfere with the medical quality review functions performed by the NQMC. In addition, individuals do not require an opportunity to consent, because federal law protects the confidentiality of records examined by the NQMC for both beneficiaries and health care providers. With respect to beneficiaries, quality assessment and improvement activities fall within the definition of healthcare operations under the HIPAA Privacy Rule as implemented by DoD 6025.18-R, DoD Health Information Privacy Regulation. That regulation permits TRICARE, as a covered entity under HIPAA, to use or disclose PHI of MHS beneficiaries for its own healthcare operations. Beneficiaries are not entitled to object to information collection for such a permitted use or disclosure of PHI. With respect to health care providers, 10 USC sec. 1102 as implemented by DoD 6025.13-R, C2 protects the confidentiality of medical quality assurance records created by or for the DoD as part of a medical quality assurance program. Therefore, PII contained in DoD medical quality assurance records is generally protected from disclosure.

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.

MAXIMUS NQMC does not collect PII directly from individuals.



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.