



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Collection and Analysis Software
(Remark® Office Optical Mark Recognition (OMR))

US Army Medical Command - Defense Health Program (DHP) Funded Application

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 219, Protection of Human Subjects; 21 CFR 56, Institutional Review Boards; DoDI 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD Supported Research; DoDI 6000.08, Defense Health Program and Clinical Investigation Programs.

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 Gravic Remark Office Optical Mark Recognition (OMR) is a software product for collecting and analyzing data from tests, surveys, assessments, evaluations, and other plain paper forms. It operates on a Windows workstation and data is input onto the workstation via a scanner. When a survey or document is scanned, the software recognizes optical marks on the page and converts it to numeric data (based on rules predefined by the user) in the form of a spreadsheet linked to the scanned images. The scanned images and the resulting spreadsheet data can be exported in a variety of formats.

Some research programs within the US Army Medical Command use Remark Office OMR to import and organize survey responses from the paper surveys they administer. The data collected is stored in the Remark Office OMR software and retained in a limited access file indefinitely. The types of PII collected and stored include the individual's gender, mother's maiden name, and marital status.

(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 collection, use, and storage of PII are unauthorized access and unauthorized disclosure. Administrative, technical, and physical security measures are in place to mitigate these risks as mentioned in Section 3 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.

The PII will be shared with authorized research investigators within the US Army Medical Command research program using this software.

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.

There are some staff who are employed in a contractual basis. There are clauses in their contracts requiring compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) requirements to protect the confidentiality

of personal information.

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.

The PII collected in the Remark Office file is collected from the surveys being scanned. The survey participants receive an information sheet approved by the Institutional Review board (IRB) as part of the research study protocol that provides the specific information relevant to the survey being conducted. This information sheet states that participation in the survey is voluntary. Individuals can object to the collection of PII by not participating in the study or not providing the PII elements requested in the study. There are no consequences if individuals do not participate in the study or fail to provide their PII.

(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.

The PII collected in the Remark Office file is collected from the surveys being scanned. The survey participants receive an information sheet approved by the Institutional Review board (IRB) as part of the research study protocol that provides specific information relevant to the survey being conducted. This information sheet outlines how PII will be used and provides an opportunity for individuals to withhold or consent to the specific uses of their PII. Individuals who do consent to the specific uses can opt out of participating in the study or providing the PII elements requested in the study. There are no consequences if individuals do not participate in the study or fail to provide their PII.

(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.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

An information sheet is provided to each participant in the survey. This information sheet is approved by the Institutional Review board (IRB) as part of the research study protocol and provides specific information relevant to the survey being conducted. The information sheet addresses the following:

- Principal purpose of the study
- Use of data collected
- Design of the assessment
- Risk and discomforts to the participant
- Whether disclosure of PII is mandatory or voluntary
- Effect on individuals of not providing their PII

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.