



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Health Information Portal (HIP, formerly eGUI)
--

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.

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 55, Medical and Dental Care; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 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.

In the 3rd Quarter of Fiscal Year 2010, Defense Health Information Management Systems (DHIMS) began development of the Enterprise Graphical User Interface (EGUI). Prior to deployment, functional users requested the name of the EGUI change to something indicative of the system's intended use. It was decided that Health Information Portal (HIP) adequately described the new application and thus the name was officially changed.

HIP is an initial step in the modernization of the Military Health System (MHS) digital user interface, allowing multiple health systems to be condensed into one platform for efficient viewing and improved patient care. HIP will be centrally hosted within the enterprise and users will access HIP as a web application with authentication. This access will provide a web-based view of data aggregated from multiple MHS and Veterans Affairs (VA) systems through the Bidirectional Health Information Exchange 5 (BHIE 5) data framework. BHIE 5 enhanced legacy BHIE by improving speed and adding web service capabilities. BHIE provides data from the Clinical Data Repository (CDR), Theater Medical Data Store (TMDS), the VA's Health Data Repository (HDR), Veterans Health Information Systems and Technology Architecture (VistA), Essentris, Composite Health Care System (CHCS), Health Artifact and Imaging Management Solution (HAIMS), and the Neuro-Cognitive Assessment Tool (NCAT).

HIP displays patient records in the following areas: Allergies, Assessments, Appointments – Outpatient, Encounters, HAIMS Artifacts and Images, Histories, Joint Registration (Federal Health Care Center (FHCC) Only), Lab Flow Sheet, Lab Results, Links, Medications – Inpatient (DoD Only), Medications – Outpatient, My Page, My Recent Patients, Patient Banner, Patient Demographics, Patient Notes, Patient Search, Problem List, Procedures, Questionnaires, Radiology, Site Monitor, Vitals.

Personally identifiable information (PII) and protected health information (PHI) is disseminated (not collected or maintained with the exception of the My Recent Patients portlet) to allow providers to access patient records in a seamless customizable view.

The My Recent Patients portlet is the only portlet that maintains patient information. This portlet provides a viewing history and quick access to recently searched patient records. My Recent Patients is defaulted to display patients searched for in the past thirty days. If desired by the user, the portlet can be configured to a longer time span. The personal information displayed (My Recent Patients portlet) in this system is as follows:

- Name
- Gender
- Birth Date
- Age
- Military Record (Rank)
- Family Member Prefix (FMP)/Sponsor Social Security Number (SSN)

Disseminated information (the information is sent from BHIE and displayed in a read only view within HIP). This information is not stored or cached like the My Recent Patients portlet:

- Name
- Other names used
- SSN
- Legal status
- Gender
- Race/Ethnicity
- Birth date
- Place of birth
- Personal cell telephone number
- Home telephone number
- Mailing/Home address
- Religious preference

- Mother's maiden name
- Mother's middle name
- Spouse information
- Marital status
- Child information
- Financial information
- Medical information
- Disability information
- Employment information
- Military record (Rank)
- Emergency contact
- FMP

The information stored in this system consists of PII protected by the Privacy Act of 1974, as amended, and PHI protected by Health Insurance Portability and Accountability Act of 1996 (HIPAA). The individuals whose information is stored in this system include active duty military (all services plus Coast Guard and Reserve), spouses, dependents, veterans, retirees and their spouses/dependents.

The system is located at the James A. Lovell Federal Healthcare Center in North Chicago and Defense Information Systems Agency (DISA). HIP is accessed by users affiliated with Defense Health Information Management System (DHIMS), North Chicago and by users who are members of the MHS Active Directory.

The system is only accessible as a website, but not accessible by the public.

The point of contact for the system is:
 Program Manager, DHIMS
 5111 Leesburg Pike, Suite 817
 Falls Church, VA 22041
 (703) 998-6900

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

HIP is susceptible to the same privacy risks inherent in any system collecting, using, and sharing PII / PHI. If this system is not properly protected, then the PII/PHI contained therein could be accessed by unauthorized individuals through various methods such as data interception, unauthorized access, internal threats and external threats.

Access to HIP is monitored and limited to users who are a part of the MHS Active Directory which is controlled and monitored by Military Health System Cyberinfrastructure Services (MCIS). Unauthorized access is mitigated by limiting the access to PII / PHI to trusted individuals only; these individuals have an Automatic Data Processing / Information Technology (ADP/IT)-II Position Category clearance as defined by DoD 5200.2-R and DoDI 8500.2 and must be a member of the database in order to access the data. External threats are mitigated by following DISA provided checklists as part of the HIP Accreditation efforts under the DoD Information Assurance Certification & Accreditation Program (DIACAP). This ensures that all necessary checks are followed to maintain the security of the HIP system.

All applicable security and privacy processes and regulations (including DIACAP, Privacy Act, and HIPAA training for all users) required of a DoD system in operation are defined and implemented, reducing risks to the maximum extent possible and to the point that any remaining risk has been accepted by the HIP Designated Approving Authority (DAA). The HIP received its ATO on 23 September 2010 and is currently participating in its annual review.

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.

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

Individuals cannot object because the collection of PII / PHI has already been done prior to any PII / PHI being accessed by the HIP servers. The HIP servers have a system-to-system interface with several DoD and VA systems using the BHIE 5 data framework.

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.

Individuals cannot object because the collection of PII / PHI has already been done prior to any PII / PHI being accessed by the HIP servers. The HIP servers have a system-to-system interface with several DoD and VA systems using the BHIE 5 data framework.

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 type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

HIP is not the initial point of collection of PII and/or PHI; therefore, no privacy act statement or privacy advisory is required.

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.