



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Computerized Biofeedback System (Mind Media BioTrace+/NeXus-10)

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

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
- 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.

10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

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 Nexus 10 can be used for all kinds of biofeedback and neurofeedback applications by measuring a wide variety of signals such as brainwaves (EEG), muscle tension, heart rate, relative blood flow, skin conductance, respiration, and temperature. The purpose of the system is to treat a variety of clinical conditions (e.g., anxiety, headaches). The NeXus 10 comes with the easy to use and highly customizable BioTrace+ software. BioTrace+ is a complete software package for physiological monitoring and a wide range of biofeedback and neurofeedback applications used to set up treatment protocols with patients. All categories of DoD health care beneficiaries may have records in this system.

This software application collects the following personal information: Name, Gender, Race/Ethnicity, Marital Status, and Medical Information.

(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 PII collection are unauthorized access, inaccurate information in the system, and unauthorized disclosure of PII. There are physical, technical, and administrative security safeguards in place to mitigate these risks. These safeguards are addressed 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.

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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review and signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and will become a permanent part of the health care record. If the individual objects to the collection of their PII, comprehensive health care may not be possible, but care is not denied.

(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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review and signature. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and will become a permanent part of the health care record. If the individual objects to the specific uses of their PII, comprehensive health care may not be possible, but care is not denied.

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

Describe each applicable format.

DEPARTMENT OF DEFENSE (DD) FORM 2005, PRIVACY ACT STATEMENT – HEALTH CARE RECORDS

1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN)
Sections 133, 1071-87, 3012, 5031 and 8012, title 10, United States Code and Executive Order 9397.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED
This form provides you the advice required by The Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.

3. ROUTINE USES
The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to: Aid in preventive health and communicable disease control programs and report medical conditions required by law to federal, state and local agencies; compile statistical data; conduct research; teach; determine suitability of persons for service or assignments; adjudicate claims and determine benefits; other lawful purposes, including law enforcement and litigation; conduct authorized investigations; evaluate care rendered; determine professional certification and hospital accreditation; provide physical qualifications of patients to agencies of federal, state, or local government upon request in the pursuit of their official duties.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION
In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other personnel/ beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED. This all inclusive Privacy Act Statement will apply to all requests for personal information made by health care treatment personnel or for medical/dental treatment purposes and will become a permanent part of your health care record.
Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|---|---|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input type="checkbox"/> Social Security Number (SSN) |
| <input checked="" type="checkbox"/> Truncated SSN | <input type="checkbox"/> Driver's License | <input type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Legal Status | <input type="checkbox"/> Gender |
| <input type="checkbox"/> Race/Ethnicity | <input type="checkbox"/> Birth Date | <input type="checkbox"/> Place of Birth |
| <input type="checkbox"/> Personal Cell Telephone Number | <input type="checkbox"/> Home Telephone Number | <input type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input type="checkbox"/> Spouse Information |
| <input type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Medical Information | <input type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Employment Information | <input type="checkbox"/> Military Records |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Education Information | <input type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

The PII is collected directly from the individual for this system.

(3) How will the information be collected? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input type="checkbox"/> Information Sharing - System to System | |
| <input checked="" type="checkbox"/> Other | |

PII is obtained from the patient and manually entered into the system.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

PII is collected for the verification and identification of the patient and/or their sponsor in order to match the proper individual with their respective medical records and reports.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

The intended use of the PII collected is for administrative and mission-related to support the delivery of health care services.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

- Yes No

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

- Users** **Developers** **System Administrators** **Contractors**
- Other**

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> Cipher Locks |
| <input checked="" type="checkbox"/> Identification Badges | <input type="checkbox"/> Combination Locks |
| <input type="checkbox"/> Key Cards | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input type="checkbox"/> Safes | <input type="checkbox"/> Other |

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

- | | |
|---|--|
| <input checked="" type="checkbox"/> User Identification | <input type="checkbox"/> Biometrics |
| <input checked="" type="checkbox"/> Password | <input checked="" type="checkbox"/> Firewall |
| <input type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Virtual Private Network (VPN) |
| <input checked="" type="checkbox"/> Encryption | <input type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input type="checkbox"/> External Certificate Authority (CA) Certificate | <input checked="" type="checkbox"/> Common Access Card (CAC) |
| <input type="checkbox"/> Other | |

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

- Periodic Security Audits**
- Regular Monitoring of Users' Security Practices**
- Methods to Ensure Only Authorized Personnel Access to PII**
- Encryption of Backups Containing Sensitive Data**
- Backups Secured Off-site**
- Other**

Personnel complete DoD Cyber Security Awareness, Privacy Act, and Health Insurance Portability and Accountability Act (HIPAA) training on an annual basis.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

- | | | | |
|--------------------------|--|----------------------|----------------------|
| <input type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | <input type="text"/> |

No, this DoD information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: Will only collect relevant PII on individuals as required for the intent of this system. Data will be unclassified/sensitive/FOUO only. PII will be protected and file permissions restrict access to data by authorized personnel only. Users are trained in the use and protection of PII, PHI, and FOUO data.
Use: Will use the PII collected only for the intended purpose of this system. Only personnel with a need-to-know can access the data. The use of firewalls, authentication, and encryption will be used to secure information processed. Vulnerability assessments are conducted to ensure data is protected.
Retention: Data will be retained indefinitely. Audit trail records are retained and maintained by trained IT personnel.
Processing: While data is being processed, all available IA best practices will be adhered to. IA controls are in place to ensure data is stored, processed, and transmitted by IA approved methods.
Disclosure and Destruction: Personnel will not disclose PII to anyone other than to individuals or approved entities. Authorized destruction policies are in place.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Not applicable

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

There are sufficient physical, technical, and administrative safeguards, as indicated in Section 3d, to mitigate all known privacy risks.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

GRILLS.CHAD.E.1271290612
Digitally signed by GRILLS.CHAD.E.1271290612
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA,
cn=GRILLS.CHAD.E.1271290612
Date: 2015.01.07 08:20:03 -10'00'

Name: Chad Grills, Ph.D.

Title: OIC, Brain Injury Clinic

Organization: USAHC-SB

Work Telephone Number: 808-433-8139

DSN:

Email Address: chad.e.grills.civ@mail.mil

Date of Review: 1/7/2014

Other Official Signature (to be used at Component discretion)

LOHMAN.
FRANK.B.
11706849
46
Digitally signed by: LOHMAN.FRANK.B.1170684946
DN: CN = LOHMAN.FRANK.B.1170684946 C = US
O = U.S. Government OU = DoD
Date: 2015.01.09 14:43:44 -09'00'

Name: Frank B. Lohman

Title: PRMC IAM

Organization: PRMC / TAMC

Work Telephone Number: (808) 433-5033

DSN: 315-433-5033

Email Address: Frank.B.Lohman.civ@mail.mil

Date of Review: 2015 01 09

**Other Official Signature
(to be used at Component
discretion)**

**MESA.GREGORY.E.1184
391224** Digitally signed by MESA.GREGORY.E.1184391224
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USA, cn=MESA.GREGORY.E.1184391224
Date: 2015.01.09 14:50:41 -10'00'

Name: Gregory Mesa

Title: Freedom of Information / Privacy Act Officer

Organization: Tripler Army Medical Center

Work Telephone Number: (808) 433-4663

DSN:

Email Address: gregory.e.mesa.civ@mail.mil

Date of Review: 9 January 2015

**Component Senior
Information Assurance
Officer Signature or
Designee**

Ashley Dale Digitally signed by Ashley Dale
DN: cn=Ashley Dale, o=Defense Health
Agency - HQ MEDCOM, ou=HQ MEDCOM
IA, email=ashley.e.dale.civ@mail.mil, c=US
Date: 2015.01.22 11:14:57 -08'00'

Name: Ms. Ashley E. Dale

Title: Acting Information Assurance Program Manager

Organization: Headquarters, US Army Medical Command

Work Telephone Number: 210-834-5335

DSN: NA

Email Address: ashley.e.dale.civ@mail.mil

Date of Review:

**Component Privacy Officer
Signature**

**PETERSON.JOHN.PHILLIP.1
014148619** Digitally signed by PETERSON.JOHN.PHILLIP.1014148619
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA,
cn=PETERSON.JOHN.PHILLIP.1014148619
Date: 2015.01.22 14:03:24 -06'00'

Name: Mr. John P. Peterson

Title: Chief, Privacy Act/FOIA Office

Organization: Headquarters, US Army Medical Command

Work Telephone Number: 210-221-4322

DSN: 471-4322

Email Address: john.p.peterson.civ@mail.mil

Date of Review: 22 January 2015

**Component CIO Signature
(Reviewing Official)**

TUCKER.DAVID.W.1039797
042

Digitally signed by TUCKER.DAVID.W.1039797042
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=USA, cn=TUCKER.DAVID.W.1039797042
Date: 2015.01.23 14:57:12 -05'00'

Name:

For LTC Richard A. Wilson

Title:

Chief Information Officer/G6

Organization:

Office of The Surgeon General/Headquarters, US Army Medical Command

Work Telephone Number:

703-681-8286

DSN:

761-8286

Email Address:

richard.a.wilson34.mil@mail.mil

Date of Review:

23 January 2015

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.