PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Interagency Comprehensive Plan for Care Coordination Support (ICPCCS)

2. DOD COMPONENT NAME:

Defense Health Agency

Program Executive Office (PEO) Medical Systems (J-6)

3. PIA APPROVAL DATE:

07/14/23

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees
- [x] from both members of the general public and Federal employees
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Interagency Comprehensive Plan for Care Coordination Support (ICPCCS) application supports the Recovery Coordination Program's chief mission which is to improve the care, management, and transition of Recovering Service Members (RSM). Contact information is used by Recovery Care Coordinators to facilitate the uniformity and effectiveness of care and transition from active duty to temporary or permanent retirement for eligible individuals. These records are also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research. ICPCCS users include the entire community of personnel who perform care coordination and case management work for wounded, ill, or injured Service Members and Veterans (SM/Vs). ICPCCS is a web based application that is accessible via the Internet that is accessible to personnel operating out of Military Treatment Facilities (MTFs). However, only authorized users are able to access ICPCCS as users are authenticated by their Common Access Card (CAC) so it is limited to DoD personnel only. ICPCCS is currently being hosted at the Defense Information Systems Agency (DISA) location in Mechanicsburg, PA.

Personally identifiable information (PII) and protected health information (PHI) collected includes Employment Information, Home/Cell Phone, Mailing/Home Address, Military Records, Official Duty Address, Race/Ethnicity, Work E-mail Address, Birth Date, Disability Information, Education Information, Financial Information, Marital Status, Official Duty Telephone Phone, Personal E-mail Address, Position/Title, Rank/Grade, Security Information, Child Information, DoD ID Number, Emergency Contact, Gender/Gender Identification, Legal Status, Medical Information, Name(s), PHI, Religious Preference, and Social Security Number (SSN) information.

PII is collected from the following categories of individuals: Active Duty Service Members, Veterans, authorized DoD beneficiaries, Federal employees, and members of the general public (i.e. federal contractors).

ICPCCS is owned and operated by the Care & Benefits Integrated Systems (CBIS) Program Management Office (PMO)/Solution Delivery Division (SDD)/Program Executive Office (PEO) Medical Systems (J-6)/Defense Health Agency (DHA).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected for verification and mission-related use. The intended use of collected PII is to improve the care, management, and transition of injured Service members and Veterans.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Participation in the Recovery Coordination Program (RCP) is voluntary. Individuals may verbally object to the collection of their PII upon

contact with the Recovery Care Coordinator (RCC); however, individuals who choose not to provide the requested information may face significant administrative delay(s) or loss of services that might otherwise be avail ble.

f. Do individuals have the opportunity to consent to the specific uses of their PII? X 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.

Participation in the Recovery Coordination Program (RCP) is voluntary. Individuals may verbally consent to the specific uses of their PII upon contact with the Recovery Care Coordinator (RCC); however, individuals who choose not to provide the requested information may face significant administrative delay(s) or loss of services that might otherwise available.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

X Privacy Act Statement Privacy Advisory Not Applicable

The participant is advised of the Privacy Act when entering into the program for treatment. The participant at this time has the right to refuse providing information into the system.

Authorities: 10 U.S.C. 113, Secretary of Defense; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); DoD Instruction 1300.24, Recovery Coordination Program (RCP); and E.O. 9397, (SSN) as amended.

Purpose(s): To improve the timeliness, efficacy, and transparency of the care, management, and transition of RSMs or eligible family members and caregivers receiving support (as defined in DoD Instruction 1300.24). Contact information is used by case managers to facilitate the uniformity and effectiveness of care and/or transition from active duty to temporary or permanent retirement for eligible individuals. These records are also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

Routine Use(s): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Service member records are shared with the Department of Veterans Affairs (VA) as a check list upon completion of the program with the DoD.

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure: Voluntary; however, failure to provide identifying information may negatively impact the services provided to him/her if they object to providing this information. The SSN is collected to afford retrieval of demographic information for records necessary to ensure the completed information is filed properly to support the Service member transitioning from recovery and rehabilitation.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

x	Within the DoD Component	Specify.	Office of Warrior Care Policy
x	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	The Departments of the Army, Navy, Air Force, Marine Corps, and Special Operations Combatant Command (SOCOM)
x	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	The Department of Veterans Affairs (VA) and the Department of Homeland Security (DHS)-U.S. Coast Guard
	State and Local Agencies	Specify.	
x	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Syneren Technologies - System Vendor and Developer Both contracts specify a Non-Disclosure Agreement (NDA) signed by all employees assigned to the contract to protect PII, Privacy Act Information and beneficiary's rights under HIPAA. No FARs are referenced in the contract but several DoD Directives and Regulations are: Namely; DoDM 6025.18; DoD 5400.11; DoDI 8500.01; and DoDM 5200.02-R. All data is managed and maintained by the software vendor(s). They are occasionally required to access this information to address trouble tickets from the users to provide help desk support for access and data issue resolution. No PII is ever downloaded or removed from ICPCCS, or shared with contractor-owned systems. Contractors are only able to access and view the data while logged into ICPCCS with a CAC on a GFE. Per their contract, the contractors are required to: "…establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of Government data. As a minimum, this shall include provisions for Program/System Security, Risk Management Framework Support, Information Assurance Vulnerability management (IAVM), Public Key Infrastructure, Physical Security, Personnel Security, Security Design and Configuration, Identification and Authentication, Enclave and Computing Environment, Physical and Environmental, Continuity, Vulnerability and Incident as listed."
	Other *(e.g., commercial providers, colleges)*.	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

x	Individuals	x	Databases
x	Existing DoD Information Systems		Commercial Systems
x	Other Federal Information Systems		

Individuals: Service Members.
Existing DoD Information Systems: Defense Enrollment Eligibility Reporting System (DEERS); Defense Casualty Information Processing System (DCIPS).
Other Federal Information Systems: Total Force Data Warehouse (TFDW).
Databases: Operational Data Store Enterprise (ODSE).

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

x	E-mail	x	Official Form (*Enter Form Number(s) in the box below)*
x	In-Person Contact	x	Paper
x	Fax	x	Telephone Interview

x Information Sharing - System to System x Website/E-Form

x Other *(If Other, enter the information in the box below)*

Official Forms: DD Form 2948; DD Form 93; DD Form 214; DD Form 2860; DD Form 2870; DD Form 2656; AF Form 356; VA Form 10-0454.
Website/E-Form: https://rcpss.csd.disa.mil/rcpss/.
Information Sharing - System to System: DEERS; Federal Case Management Tool (FCMT)
Other: DoD Secure Access File Exchange (SAFE).

k. 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 must be consistent.

x Yes No

If "Yes," enter SORN System Identifier DPR 40 DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-0330-2015-0003-0001

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

FILE NUMBER: 1805-28 FILE TITLE: Recovery Coordination Program Support Solution (RCP-SS) Disposition: Cut off annually, after the separation/retirement of the service member or termination/retirement of the civilian servant. Destroy 10 year(s) after cut off.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 113, Secretary of Defense; DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); DoD Instruction 1300.24, Recovery Coordination Program (RCP); and E.O. 9397, (SSN) as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 x No Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

As participation in the Recovery Coordination Program (RCP) is voluntary, ICPCCS is not subject to the Paperwork Reduction Act (PRA) per DoDM 8910.01: "DoD Information Collections Manual: Procedures for DoD Public Information Collections," Volume 2, Enclosure 3, Section 8(a1): "Public Information Collections Addressed to Nine or Fewer Persons.