

## PROCEDURES FOR OBTAINING AN ACCOUNT FOR THE NAVY'S DISEASE REPORTING SYSTEM-INTERNET (DRSi)

**INTRODUCTION:** Due to Health Insurance Portability and Assurance Act (HIPAA) and Privacy Act requirements, the Navy and Marine Corps Public Health Center requires assurance from the requesting command or unit that access to sensitive personal and health information will be protected.

### **Completing and Submitting DD Form 2875**

Preferably, one primary and one secondary MER Recorder should be assigned to each Navy Medical Department. One form per person must be sent to the Navy's DRSi Helpdesk.

#### **1. USER (requesting access)**

- Complete blocks 1-12 (Part I).
- CAC signature of the requester is needed for block 11 (*Block 10 must be completed or CAC signature will not save*).
- In block 13, annotate the REPORTING UNIT(s), (UIC or DMIS ID for Navy and OPFAC for Coast Guard and the COMMAND NAME(s) of the CLINIC or FACILITY for which you will report or monitor Medical Event Reports. Regional NEPMU account requestors should provide the NEPMU Name and NEPMU Reporting UIC).
- ***Forms forwarded to the Helpdesk without the Reporting Unit(s) and the Name of the Clinic or Facility will delay processing and access.***
- ***Send the form to someone in your chain of command who can fill out the SUPERVISOR section in step #2 below. This person must be a DEPARTMENT HEAD or someone delegated "BY-DIRECTION" authority or higher (no exceptions).***
- Users, who will **TRANSFER** to another command, should contact the Helpdesk so the current Reporting Unit can be deactivated. If access to Navy DRSi is needed at the new command, you must submit a **NEW** request and have it endorsed by your new leadership.
- Users who will **RETIRE or SEPARATE** should contact the Helpdesk so their account can be deactivated.

#### **2. SUPERVISOR**

- In Block 13, verify that the Reporting Unit(s) is the correct Reporting Unit(s) for which the individual will report or monitor Medical Event Reports.
- Blocks 16-20b, **must be a DEPARTMENT HEAD or someone delegated "BY-DIRECTION" authority or higher (no exceptions).**
- CAC signature is needed for block 18 (Block 17, 19 and 20-20b must be completed or CAC signature will not save).

#### **3. FORWARDING COMPLETED SAAR:**

There are several ways the completed SAAR can be forwarded to the Helpdesk. If these options do not meet your current IT/communication environment, please contact the Navy DRSi Helpdesk via email [ndrs@nmcphe.med.navy.mil](mailto:ndrs@nmcphe.med.navy.mil) or via phone at 757.953.0954/DSN: 377.0954.

- a. **EMAIL-** if forms are received with Reporting Unit information in block 13 and electronic signatures for Part I and Part II, the Helpdesk will activate the account immediately and the Requestor will receive their login id and initial password via e-mail.
- b. **FAX-** once a form is received, the Helpdesk will forward an e-mail to the endorser in block 16-20b, per DOD regulations, for verification purposes. The endorser must respond via e-mail approving access. Once verified, the Requestor will receive their login id and initial password via e-mail from the Helpdesk to access Navy DRSi.
- c. **U.S. Mail-** send a complete SAAR form to include in block 13 the Reporting Unit and Name of Clinic or Facility to the below address. The Helpdesk will forward an e-mail to the endorser in block 16-20b, per DOD regulations, for verification purposes. The endorser must respond via e-mail approving access. Once verified, the Requestor will receive their login id and initial password via e-mail from the Helpdesk to access NDRSi.

Navy and Marine Corps Public Health Center  
(Attn: NDRSi Helpdesk)  
620 John Paul Jones Circle Suite 1100  
Portsmouth, VA 23708

As of July 2012

## SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

### PRIVACY ACT STATEMENT

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.  
**PRINCIPAL PURPOSE:** To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.  
**ROUTINE USES:** None.  
**DISCLOSURE:** Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____	DATE (YYYYMMDD)
---	-----------------

SYSTEM NAME (Platform or Applications) Naval Disease Reporting System internet (NDRSi)	LOCATION (Physical Location of System) NMC Public Health Center
---	--

**PART I (To be completed by Requestor)**

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE (DSN or Commercial)
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER
9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR	
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training.    DATE (YYYYMMDD) _____	
11. USER SIGNATURE	12. DATE (YYYYMMDD)

**PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)**

13. JUSTIFICATION FOR ACCESS  
 The Requestor agrees to comply with block 27. Please provide the Reporting Unit of the location for the clinic which you report or need visibility along with the name of the Facility."

FAX FORM TO: 757-953-0685 (DSN 377-0685)  
 The Requestor agrees to comply with block 27.

14. TYPE OF ACCESS REQUIRED:  
 AUTHORIZED     PRIVILEGED

15. USER REQUIRES ACCESS TO:     UNCLASSIFIED     CLASSIFIED (Specify category)  
 OTHER Sensitive medical information

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)
---	--

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
------------------------------------	----------------------------	---------------------

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
--	----------------------------------	-------------------

21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
--	-------------------	----------------------

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)
-----------------------------------	-----------------------------	------------------	---------------------

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional information)  
 I understand that to ensure the integrity, safety and security of Navy IT resources, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- Protect Controlled Unclassified Information (CUI) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect passwords for systems requiring logon authentication and safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- Virus check all information, programs, and other files prior to uploading onto any Navy IT resource.
- Report all security incidents immediately in accordance with local procedures and CJCSM 6510.01 (series).
- Access only that data, control information, software, hardware, and firmware for which I am authorized access and have a need-to-know, and assume only those roles and privileges for which I am authorized.
- Be subject to monitoring, and further understand that there is no expectation or right to privacy over the data and communications generated through my use. - Understand the information I'm viewing is for Official Use Only. Any misuse/unauthorized disclosure can result in civil/criminal penalty. I further understand that, when using Navy IT resources, I shall not:- Access commercial web-based e-mail (e.g. HOTMAIL, YAHOO!, AOL, etc.)
- Auto-forward official e-mail to a commercial e-mail account.
- Bypass, strain, or test IA mechanisms (e.g., Firewalls, content filters, anti-virus programs, etc.). If IA mechanisms must be bypassed, I shall coordinate the procedure and receive written approval from the Local IA Authority (CO or OIC).
- Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource.
- Relocate or change equipment or the network connectivity of equipment without authorization from my Local IA Authority.
- Use personally owned hardware, software, shareware, or public domain software without authorization from the Local IA Authority. - Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of the Local IA Authority.- Participate in or contribute to any activity resulting in a disruption or denial of service.
- Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
- Put Navy IT resources to uses that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service).

**PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION**

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNINATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)

**PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION**

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)

## INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

**A. PART I:** The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (5) Official E-mail Address. The user's official e-mail address.
- (6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
- (7) Official Mailing Address. The user's official mailing address.
- (8) Citizenship (US, Foreign National, or Other).
- (9) Designation of Person (Military, Civilian, Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (12) Date. The date that the user signs the form.

**B. PART II:** The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)
- (15) User Requires Access To: Place an "X" in the appropriate box. Specify category.
- (16) Verification of Need to Know. To verify that the user requires access as requested.
- (16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (19) Date. Date supervisor signs the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) E-mail Address. Supervisor's e-mail address.
- (20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

**C. PART III:** Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

**D. PART IV:** This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

### E. DISPOSITION OF FORM:

**TRANSMISSION:** Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

**FILING:** Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.