

PROCEDURES FOR OBTAINING **USER** ACCOUNTS FOR THE NAVY AND MARINE CORPS PUBLIC HEALTH CENTER (NMCPHC) NAVAL DISEASE REPORTING SYSTEM-INTERNET (NDRSi)

INTRODUCTION: Due to Health Insurance Portability and Assurance Act (HIPAA) and the 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.

A copy of the DD Form 2875 System Authorization Access Request (SAAR) can also be downloaded from NMCPHC's website at http://www-nmcphc.med.navy.mil/prevmed/epi/Reporting_Tools.htm, or request by e-mailing the NDRS HelpDesk at ndrs@nehc.med.navy.mil.

Special Instructions for Completing and Submitting **DD Form 2875**

One form per account user must be sent to NMCPHC. This form consists of two pages with information and one page of instructions. Once the form is verified, NMCPHC will activate the user account via phone or e-mail. Users will then sign in and set up their profile and account.

- "User" is defined as anyone requesting access to the NDRS internet system.
- 1. NDRSi users are to complete Part I and initial block 27. **Part II must be completed and signed by a Supervisor delegated with "By Direction" authority of the Unit Commander, such as a department head or higher. For US Coast Guard, this will be the CHSD or DMOA.** Blocks 21 – 25 and all of Part's III and IV may be excluded.
- 2. Users will also need to notify NMCPHC of when they will leave, transfer, or no longer require access so that their account may be terminated or changed to new location. Military members and Contractors are to specify their PRD or contract expiration date in block 16a.
- 3. Forms will be maintained by the NDRS Administrator.

Users may send the DD-2875 by one of the following methods below. If these options do not meet your current IT/communications environment, please contact the NDRS HelpDesk at ndrs@nehc.med.navy.mil or by phone at 757-953-0954/DSN 377-0954:

- a. **FAX** – NMCPHC will contact the official listed in Part II to verify the request and activate the NDRS user account (FAX: **757-953-0685** or DSN 377-0685).
- b. **E-MAIL** – Complete, sign, and scan the form to ndrs@nehc.med.navy.mil. Because the form includes personal information, the form must be sent by encrypted e-mail or as a password protected file. The password should be called in or sent in separate e-mail.
 - * If form is sent by the signing official in Part II, NMCPHC will activate the local user account immediately. If sent by the user, NMCPHC will need to contact the signing official for verification and will not activate the account until such verification is provided.
- c. **MAIL** – NMCPHC will contact the official listed in Part II to verify the request and activate the user account. Mail form to:
 - Navy and Marine Corps Public Health Center
 - Attn: NDRS HelpDesk
 - 620 John Paul Jones Circle, Suite 1100
 - Portsmouth, VA 23708

*****If you haven't received a response within 24hrs, please call the HelpDesk at 757-953-0954 or 757-953-0717*****

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 Social Security Numbers 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 | | DATE (YYYYMMDD) |
| <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID | | |
| SYSTEM NAME <i>(Platform or Applications)</i> | | LOCATION <i>(Physical Location of System)</i> |

PART I (To be completed by Requestor)

| | | |
|--|---|---|
| 1. NAME <i>(Last, First, Middle Initial)</i> | | 2. SOCIAL SECURITY NUMBER |
| 3. ORGANIZATION | 4. OFFICE SYMBOL/DEPARTMENT | 5. PHONE <i>(DSN or Commercial)</i> |
| 6. OFFICIAL E-MAIL ADDRESS | | 7. JOB TITLE AND GRADE/RANK |
| 8. OFFICIAL MAILING ADDRESS | 9. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER | 10. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR |

USER AGREEMENT

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.)

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

14. TYPE OF ACCESS REQUIRED:
 AUTHORIZED PRIVILEGED

15. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED *(Specify category)*
 OTHER _____

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

| | | |
|---|-----------------------------------|----------------------------|
| 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) |
|--|------------------------------------|-------------------------|----------------------------|

| | |
|---|-----------------------------|
| 26a. NAME (Last, First, Middle Initial) | 26b. SOCIAL SECURITY NUMBER |
|---|-----------------------------|

27. OPTIONAL INFORMATION (Specify Privilege Level desired. DVS Facilitators/Schedulers - list ALL your Site IDs. See instructions for details.)

~~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 DESIGNATION <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) Social Security Number. The social security number of user.
- (3) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (4) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (5) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (6) Official E-mail Address. The user's official e-mail address.
- (7) 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.
- (8) Official Mailing Address. The user's official mailing address.
- (9) Citizenship (US, Foreign National, or Other).
- (10) Designation of Person (Military, Civilian, Contractor).

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.