DHSS COMPUTING ENVIRONMENTS

Account Authorization Request Form

DHSS COMPUTING ENVIRONMENTS Access and Security Requirements

Due to the sensitive nature of data contained within the DHSS COMPUTING ENVIRONMENTS, there are several requirements that must be satisfied before obtaining access to the system.

Requirements:

1. Non-DoD employees only: ADP-II/NACLC Clearance

2. Civilian personnel and active duty service members conducting research, non-MHS personnel and/or contractors working for the MHS/DoD: Data Sharing Agreement (DSA) on file with the Defense Health Agency (DHA) Privacy and Civil Liberties Office.

3. Department of Defense (DoD) Information Assurance (IA) Awareness Certificate on file with the DHSS PEO Access Office.

4. DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form on file with the DHSS PEO Program Office.

5. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media form– page 7 (if applicable)

1. Non-DoD employees: ADP-II/NACLC Clearance

Per DoD regulation 5200.2-R, non-DoD employees requesting access to the DHSS Computing Environments are required to have, or have submitted, a request for clearance, with a scheduled Investigation Scheduled Notice (ISN) regarding an Automated Data Processing Level II (ADP-II/NACLC), or better, position sensitivity designation. This is to give personnel an interim clearance so they can begin working with the application.

For assistance or direction on applying for an ADP-II clearance, contact your organization's Facility Security Officer (FSO). Forms and related information can be found at the OPM Web Site: http://www.opm.gov/forms/html/sf.asp

2. Civilian personnel and active duty service members conducting research, non-MHS personnel and/or contractors working for the MHS/DoD: Data Sharing Agreement (DSA)

Civilian personnel and active duty service members conducting research and non-MHS personnel and/or contractors working for the MHS/DoD requiring access to DHSS Computing Environments data are required to have a current Data Sharing Agreement (DSA) through their sponsoring organization on file with the Defense Health Agency (DHA) Privacy and Civil Liberties Office.

If you do not have a DSA please contact DHA Privacy and Civil Liberties Office at dha.ncr.health-it.mbx.dsa-mail@mail.mil

3. DoD Information Assurance Awareness Certificate

DoDD 8570.01 "Information Assurance Training, Certification, and Workforce Management", Certified Current as of April 23, 2007, requires that information system applicant/users complete Information Assurance (IA) Awareness Training on an annual basis. In accordance with this directive, the DHSS PEO Access Office must have a copy of your IA Awareness Certificate on file. Certification must be renewed annually prior to expiration in order to maintain continuous access to the DHSS COMPUTING ENVIRONMENTS. If you have not completed the DoD IA Awareness in the past year, please take the training and test by clicking *DoD IA*

Awareness (for DoD Personnel) at the following site: http://iase.disa.mil/eta. Either print or download the certificate, sign, and send it to the DHSS PEO Access Office via email at dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil. Only one valid IA Awareness Certificate is required annually, even if you have accounts on multiple DHSS PEO applications/systems.

4. DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form

A DHSS COMPUTING ENVIRONMENTS Account Authorization Request Form must be completed, signed, and e-mailed to dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil.

Requesting appropriate system area for authorized work related access:

MDR – (MHS Data Repository) Direct access to the MDR is reserved for system administrators, DHSS developers, testers, or processors. Users of the MDR access its data from the SCE Corporate or Service Node.

Corporate and/or Service Nodes – (MHS Data Repository – SAS Computing Environment) Access to the SAS Computing Environment (SCE) Corporate and/or Service Node allows read access to MDR data sets. Users of the MDR will connect from either the SCE Corporate or Service Node.

Other – List desired access to DHSS Systems beyond those listed above.

5. Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

DoD Policy Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media", July 3, 2007

References:
(a) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6. 2003
(b) DoDD 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006
(c) DoD Policy Memorandum, "Department of Defense Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
(d) DoD Policy Memorandum, "Protection of Sensitive DoD Data at Rest on Portable Computing Devices," April 18, 2006
References (a) through (c) require encryption of various categories of sensitive DoD data at rest under certain circumstances. Reference (d) provides recommendations on means to protect sensitive unclassified information on portable computing devices used within DoD and advises that the suggestions are expected to become policy requirements in the near future. This memorandum from the Department of Defense Chief Information Officer dated July 3, 2007 establishes additional DoD policy for the protection of sensitive unclassified information on mobile computing devices and removable storage media. It applies to all DoD Components and their supporting commercial contactors that process sensitive DoD information.
It is DoD policy that:
(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.

(2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c),

Encryption

- A FIPS 140-2 approved file encryption algorithm (i.e., AES, 3DES) must be used for full disk encryption to encrypt data on the remote device. Products that may be utilized include but are not limited to:
  PGP – https://www.pgp.com/products/wholediskencryption/index.html
  GuardianEdge – http://www.guardianedge.com/products/guardianedge-hard-disk-encryption.php
- Mobile computing equipment users encrypt all temporary folders (e.g., C:\temp, C:\windows\temp, Temporary Internet Files, etc.) so that any temporary files created by programs are automatically encrypted.

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI). The ESI establishes DoD-wide Enterprise Software Agreements / Blanket Purchase Agreements that substantially reduce the cost of common-use, commercial off-the-shelf software. Information on encryption products that meet the requirements of this policy may be found in Attachment 2. Other implementation details may be found at http://www.esi.mil and at http://iase.disa.mil.

Commercial vendors must provide data at rest encryption products for all mobile computing devices used to connect to DHSS products.

DHSS Computing Environments (CE) Account Authorization Request Form (AARF)

1. Please place an X to specify the system area requested for authorized work related access:

	MDR	□	**Other (specify)** ____
	Corporate Node		
	Service Node		

2a. SAS Programming Experience – Please provide your level of SAS programming skill (e.g. never used, beginner, intermediate, proficient, expert) and approximate number of years of SAS experience. If you have no SAS programming experience, you will be contacted to discuss your need for MDR access**:**

2b. What is your role in accessing the data requested?

	End User	
	Other (explain)	

3. Please specify the data requested for authorized work related access

For MDR and Corporate and Service Nodes, list Dataset names to be accessed (by node). Attach sheets if needed:

□ See attached sheet(s)

4. Employment Category ***(Please check the category that applies)***

	Government Employee, Uniformed Service Member, Military, or Civil Service working within/for DoD MHS
	Contractor working within the DoD Military Health System
	Government Employee, Uniformed Service Member, Military, or Civil Service working for other agency or directorate not a part of the DoD Military Health System
	Contractor working for Government Agency, not a part of the DoD Military Health System
	Other (Please describe) ____

5. Applicant/Requestor Information

Rank/GS Level/Title:	
Name (Last, First, MI):	
Complete Office Mailing Address:	
Sponsoring Organization Name: **(Not Project Name)**	
If Contractor, Employer Name	
Commercial Telephone Number:	
Email:	
IP Address of Workstation:	
Network Translated IP Address:	

Account Validation PIN: Enter a 4 digit numeric PIN that you will use to validate your identity for account administration purposes. **This must be the same number as entered when registering in the DHSS WebPortal.**				

6. Action

Check action requested: ❑ NEW ❑ CHANGE ❑ DELETE

If you have a User ID, please enter it here: _________________ (If your account has expired, enter your last user ID)

7A. DoD Information Assurance Awareness Training and Test (All Applicants EXCEPT MCSC)

1. Have you successfully completed the DoD Information Assurance Awareness Training and Test? □ YES □ NO
2. Have you signed and faxed the DoD Information Assurance Awareness Certificate to DHSS? □ YES □ NO

7B. Proof of DoD Information Assurance Awareness Training (MCSC ONLY)

1. Is a letter on file with DHSS verifying internal annual information assurance awareness training requirements? □ YES □ NO

8. DSA Information: If you are a Contractor please provide.

Employer Name:	
Project description requiring this access:	
What is the DUA # that exists for this project?	
Project period of performance:	

9. Applicant ADP/Security Clearance Level (mark appropriate level):

	ADP II	Notes: 1. A minimum of ADP Level II is required. 2. The use of SECRET is authorized if the requestor's clearance has been active within 2 years of application date.
	ADP I	
	Other (specify) Type __________________ Date _________________	
	If SECRET, provide: Date of Birth: __________________ Place of Birth: ____________________________	

10. Use of Mobile Computing Equipment

□ Mobile computing equipment (Laptop computer, external hard drive, CDs/DVDs, floppy disks, PDA, cell phone, or other movable media) **WILL BE USED** to connect to this DHSS product. Certification on page 10 **MUST BE COMPLETED.**

□ Mobile computing equipment **WILL NOT BE USED** to connect to this DHSS product.

11. Applicant Signature (All Applicants must read and sign)

Some data are protected under the provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA). The data contains patient and provider identity information and thus requires safeguards from unauthorized access and use. I agree to comply with the Privacy Act of 1974 and HIPAA Privacy and Security Rules and to be responsible for the use of this data to properly safeguard patient and provider identifying data. 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. *By signing below, I am acknowledging that I am only authorized to use DHSS COMPUTING ENVIRONMENTS for my current position/duty and agree to notify the DHSS PEO Access Office and relinquish my account upon departure from my current position/duty or when access is no longer required.* ***All sensitive data will be marked "For Official Use Only. The data contained is for official use only."***

Signature ____ **Date** ________________________

12. Commander, Supervisor, or Security Officer Certification of Citizenship

By signing below, I am certifying that ________________________ (applicant) is a U.S. Citizen and has a mission essential or contract-driven requirement to access the M2, and that the DUA referenced, if any, is applicable. I further acknowledge that substantial criminal penalties, including fines and imprisonment, and/or administrative sanctions may be levied against those who violate the provisions of the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act (HIPAA). I will report any change in status, duties, position, or location of the applicant that indicate that the access granted hereunder is no longer required. I shall notify the DHSS PEO Access Office upon departure of this applicant from their current position/duty or when access is no longer required.

Commander/Supervisor/Security Officer Name	
Title or Position	
Organization, Office, Company	
Office Mailing Address	
Email Address	
Commercial Telephone	

Signature ____ **Date** _________________________

13. Government Sponsor

Sponsoring Organization Name	
Commander / Supervisor / Sponsor Name (Last, First, MI)	
Title	
Office Mailing Address	
Email Address	
Commercial Telephone	
DSN	

I certify that the above named applicant requires access to the specified area(s) of the DHSS COMPUTING ENVIRONMENTS. I will report any change in status, duties, position, or location of the applicant that indicate that the access granted hereunder is no longer required.

Government Sponsor Signature ______________________________________Date ______________________

IF MOBILE COMPUTING EQUIPMENT WILL BE USED BY THIS APPLICANT, PAGE 4 MUST BE COMPLETED -- GO TO PAGE 4

= =

⦸ - - - DO NOT WRITE BELOW THIS BOX - - - ⦸

1. DHSS Certification (*For DHSS PEO use only*)

□Form □WPValidPIN □DoD IA Cert □Trng □AppSigned □CertSigned □SponSigned DHSS Access___________

I certify that DHSS requirements have been validated. Specified access is recommended.

DHSS PEO Approving Authority Name	

Signature ____ **Date** ___________________________

Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media

DoD Policy Memorandum, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media”, July 3, 2007

Per (a) DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6. 2003, (b) DoDD 8100.2, “Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG),” April 14, 2004, as supplemented by ASD NII/DoD CIO memorandum, same subject, June 2, 2006, (c) DoD Policy Memorandum, “Department of Defense Guidance on Protecting Personally Identifiable Information PII,” August 18, 2006, and (d) DoD Policy Memorandum, “Protection of Sensitive DoD Data at Rest on Portable Computing Devices,” April 18, 2006 require that:

(1) All unclassified DoD data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs), or removable storage media such as compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant and a mechanism shall be established to ensure encrypted data can be recovered in the event the primary encryption system fails or to support other mission or regulatory requirements. DoD information that has been approved for public release does not require encryption.
(2) The requirement to encrypt sensitive unclassified data at rest on mobile computing devices and removable storage media is in addition to the management and access controls for all computing devices specified in references (a) through (c).

Handling and Storage

- During travel, laptops and PDAs must be hand carried and never checked as baggage. If possible, carry diskettes or removable hard drives separate from the laptop.
- If a laptop or PDA is stored in a hotel locker room, it must be kept out of plain view. A laptop or PDA may not be left unattended in a vehicle.

Incident Handling

- In the event of any suspicious activity, breach in security of the remote device, or upon the detection of a virus, Trojan Horse, or malware disconnect from the VPN connection, cease all operation on the device, and report the incident to the DHSS IAM, Mr. Nick Saund, Narinder.S.Saund.civ@mail.mil, or the DHSS IAO, Mr. Joseph Ibanez, Joseph.G.Ibanez.civ@mail.mil.

  Please identify which mobile computing devices/removable storage media you will be using to access or obtain PHI (protected health information) from this DHSS product: (check all that apply)

□ Laptop	□ External Hard Drive	□ CDs/DVDs	□ Floppy Disks
□ PDA	□ Cell Phone	□ Other	

If other, please describe:
____

Applicant Certification: I understand the requirement for encryption of sensitive unclassified data at rest (in particular, PHI) on mobile computing devices and removable storage media. I certify that a data at rest encryption product, meeting the DoD specifications has been installed and is operating on any such mobile computing devices that I will use to access data from this DHSS product. Further, I certify that I will ensure that this data at rest encryption product shall be maintained at the most recent version and shall be kept updated according to manufacturers’ latest available patches, service packs or other product updates. Further, I will keep this product installed and operational as long as my DHSS product account is active.

Applicant Signature ____**Date** ________________________

Applicant Printed Name____

Information Assurance Manager/Information Assurance Officer Certification: I certify that I have personal knowledge of the installation and proper operation of data at rest encryption product on the above named applicant’s computer. I will ensure that required updates are applied as available.

Make and model of mobile computing device(s):

Make **Model** **Serial Number**

__________________ ____________________ _________________________

__________________ ____________________ _________________________

IAM/IAO Signature ____**Date** ________________________

IAM/IAO Printed Name____

IAM/IAO email address____**Phone** (___)__________________