SAS COMPUTING ENVIRONMENT (SCE) Account Authorization Request Form

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

	SCE Node (Basic command line access)
	SCE SAS Enterprise Guide
	Other (specify):

2. 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.

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

List either the MDR data type(s) or dataset names to be accessed. Attach additional sheets if necessary.

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

	Government Employee, Uniformed Service Member, Military, or Civil Service working within/for DoD Military Health System
	Contractor working within the DoD Military Health System (Please list organization): ____________________________________ ____
	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 *(Not Project Name)*:	
If Contractor, Employer Name:	
Commercial Telephone Number:	
Email:	
IP Address:	
Account Validation PIN (should match PIN on DD2875):	

6. Action (check action requested):

	New Account
	Change/Update Existing Account (Please list Account Name/User ID):

7. DSA Information (required for Civilian personnel and active duty service members conducting research, non-MHS personnel and/or contractors working for the MHS/DoD):

Employer Name:	
Project requiring access:	
DSA number:	
Project period of performance:	

8. 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 SDD product. *"Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media" Certification* ***MUST BE COMPLETED****.*
	Mobile computing equipment **WILL NOT BE USED** to connect to this SDD product.

9. 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 DHA SDD COMPUTING ENVIRONMENTS for my current position/duty and agree to notify the DHA SDD 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 ________________________

10. 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 MDR from the SCE, and that the DSA 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 DHA SDD PEO Access Office upon departure of this applicant from their current position/duty or when access is no longer required.

Name	
Title or Position	
Organization or Company	
Office Mailing Address	
Email Address	
Telephone	

Signature ____ Date ________________________

11. Government Sponsor	
Sponsoring Organization	
Sponsor Name	
Title or Position	
Office Mailing Address	
Email Address	
Telephone	

I certify that the above-named applicant requires access to the specified area(s) of the DHA SDD 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.

Signature ____ Date _______________________

DO NOT WRITE BELOW THIS BOX

1. SDD Certification (For DHA SDD PEO use only)

	Completed Form
	DoD Cyber Security Certificate
	Applicant Signature
	Certification of Citizenship Signature
	Sponsor Signature
	DHA SDD Access Approval

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

SDD Approving Authority	

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 DHA SDD IAM, Mr. Nick Saund, Narinder.S.Saund.civ@mail.mil , or the DHA SDD 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 SDD product: (check all that apply)

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

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 SDD 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 SDD 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 ( )_____________