Clinical Data Mart (CDM)
Account Authorization Process
Overview

CDM is the clinical reporting tool for AHLTA and equips analysts and clinicians with patient-centric data to help them identify and evaluate trends to optimize clinical performance within the MHS.

When requesting patient level data using this system, there are several requirements that must be satisfied before obtaining this level of access to CDM.

Requirements Checklist:

✓ Security Awareness Certificate on file with the EIDS Program Office

✓ CDM Account Authorization Request Form, with Commanding Officer's/Government Sponsor's certification of access level, on file with the EIDS Program Office
This includes:
- DoD Minimum Security Requirements – page 8
- PHI Justification form – page 9
- ADP/Clearance Certification – page 6
- DUA Certification – page 6 (if applicable)
- Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media form – page 10 (if applicable)

For questions or assistance with completion of these requirements, please contact the MHS Help Desk at 1-800-600-9332 (CONUS) or 1-866-637-8725 (OCONUS).

CDM – Clinical Data Mart
Account Authorization Request Form

1. Security Awareness Certificate

DoDD 8570.1 "Information Assurance Training, Certification, and Workforce Management", August 15, 2004, requires that information system users complete Security Awareness Training on an annual basis. In accordance with this directive, the EIDS Program Office must have a copy of your Security Awareness Certificate on file. Only one valid Security Awareness Certificate is required annually, even if you have accounts on multiple EIDS applications.

Instructions to access the Security Awareness Training and Testing Modules:

1. Logon to the EIDS Web site at https://eids.ha.osd.mil/ to check the currency of your Security Awareness Certificate. If you have a WebPortal Account but cannot remember your USERID or password, please contact the MHS helpdesk for assistance. DO NOT create another account on the WebPortal.
   Note: Microsoft Internet Explorer is the recommended browser.
   If you do not have an EIDS Web Account follow these steps:
   - At the EIDS Web site, select *REGISTER* from the horizontal menu bar.
   - Click *New User* on the EIDS Account Registration screen.
   - Complete the registration form and click *Register.*
   - Make note of your EIDS Web site account information.
   - Click *Login* from the EIDS Web site and log on using your EIDS Web account.
2. Click *MHS Help Desk* from the horizontal menu bar.
3. Take the Security Awareness Training by clicking *Security Awareness Training: Training Manual* (listed under *Training Modules* at the bottom of the page).
4. Take the Security Awareness Test by: (choose one)
   (a) Clicking on *Take the Security Awareness Training Exam,* listed at the end of the Manual; or
   (b) Clicking on *Security Awareness Training: Take the Test* from the MHS Help Desk screen.
5. Upon successful completion of the test, you are presented with an EIDS Security Awareness Certificate. Scroll to the bottom of the Certificate and download using the indicated link.
6. Per the form's instructions: print, sign, and fax the form to the EIDS Program Office, ATTN: EIDS Access at 866-551-1249. If you are OCONUS and having trouble with the fax, please contact the MHS Help Desk at EIDS@mhs-helpdesk.com for an alternate number.

2. DoD minimum-security requirement Certified/Compliant Workstation & Encryption for Transmission of PHI

Per DoD 8500.1, "Information Assurance (IA)," the local Commander and appointed Information System Security Officer are responsible for ensuring that automated systems under their control, that store or process unclassified sensitive data, meet minimum security standards. In certifying adherence to this requirement, the EIDS Program Office keeps a copy of DoD minimum-security requirement Certification/Compliance letters on file. This letter is page 9 of the CDM AARF.

Signed DoD minimum-security requirement Certification/Compliance letters should be faxed to the EIDS Program Office at 866-551-1249, ATTN: EIDS Access. Users should first contact their local computer network or Systems Security Officer with assistance in completing this requirement. Contact the MHS Help Desk at 1-800-600-9332 (CONUS) or 1-866-637-8725 (OCONUS) if there are any questions or concerns related to this DoD minimum-security requirement Certification.

Further, as an implementation of DoD 8580.02-R, the DoD Health Information Security Regulation EIDS requires an encrypted connection for transmission of Protected Health Information (PHI) and unclassified sensitive data. Workstation encryption status will be determined during the application process.

3. CDM Account Authorization Request Form

The CDM Account Authorization Request Form including Commanding Officer's/Government Sponsor's certification of level of access *(Pages 6-10)* must be completed, signed, and faxed to the EIDS Program Office, ATTN: EIDS Access at 866-551-1249. Listed below are items that provide further detail regarding certain requirements within the Account Authorization Request Form.

CDM – Clinical Data Mart
Account Authorization Request Form

Applicant Information. Please fill in all applicable fields. You must select a 4-digit Account Validation PIN. It may be any 4-digit number that you will remember if needed to verify your identity for account administration purposes (i.e. password reset). For instance, you may use the last 4-digits of your social security number or month and day of birth, etc. This number must be the same as the Account Validation PIN you have entered at the EIDS WebPortal: http://eids.ha.osd.mil and as provided for other EIDS systems, as applicable.

4. 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 Nil/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 of this referenced memorandum. 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 EIDS products.

Both user and organizational information security/assurance certification is required before access is granted where the user will be connecting using a mobile computing device. Completion of this certification on page 10 is required.

5. Requesting Appropriate CDM Level

With the proliferation of privacy legislation such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule the protections surrounding patient identifiable data are more stringent than ever. Safeguards will be upheld to ensure patient identifiable data is available only on a strict need-to-know basis.

One safeguard is stricter requirements for CDM access authorization. Requests for CDM roles with access to PHI will be closely scrutinized. These roles provide access to patient names, SSNs and/or pay grades. An inappropriate use and/or disclosure of this type of data could have detrimental effects on both the patient and organization. Application for roles with access to PHI require clear and detailed written justification (Page 10). The justification must include:

- Why a PHI role is critical to perform the work or the organizational mission
- The specific purpose and use of PHI in relation to the work to be performed
- If PHI is required only for the MTF where the requestor is stationed, but non patient identifiable data is needed from other areas in the MHS this must be noted in the justification. The justification must include an assurance that when querying CDM for data outside the MTF only non patient identifiable data will be accessed.

If a PHI role is required, it is highly recommended that the user also request a non-PHI role to be utilized when their reports or queries do not require patient identifiable data.

All CDM accounts are subject to random audits of use. If at any point it is discovered that the database was queried for data not covered by the justification the account will be immediately suspended pending review.

6. ADP-II/NACLC Clearance

All applicants must provide certification of proper clearance for access to a DoD Computing Network. Your Facility Security Manager or Facility Security Officer must complete all information in block 5.a., Page 6. Per DoD regulation 5200.2-R (Appendix 10 of the Personnel Security Program), non-DoD employees requesting access to CDM PHI roles 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/NACLA) or better position sensitivity designation.

7. Data Use Agreement (DUA)

The Data Use Agreement (DUA) is an organizational level document that provides permission for a particular use of the data contained in the product, for a specified period of time. The need for a DUA is dependent on several factors. First, all research uses of the data must be covered by a DUA, regardless of the users' category, including Government Employees and Uniformed Service Members. Second, all Non-MHS personnel and/or contractors working for the MHS/DoD requiring CDM roles including PHI data are required to have a current DUA. Your organization's DUA must be on file with the TRICARE Management Activity (TMA) Privacy Office. If you have questions about DUA requirements contact TMA Privacy Office at **dua.mail@tma.osd.mil**. EIDS Access Office cannot process your application without a valid DUA, if one is required. If your organization has a valid DUA, the DUA Custodian must provide information required in Block 5.b., Page 6.

CDM – Clinical Data Mart
Account Authorization Request Form

1. Employment Category (Please check the category that applies):	
	Government Employee or Uniformed Service Member working within/for DoD Military Health System
	Contractor working within/for the DoD Military Health System
	Government Employee or Uniformed Service Member working for other agency or directorate not a part of the DoD Military Health System
	Contractor working for a Government Agency, not a part of the DoD Military Health System
	Other (User must describe)

2. Applicant/Requestor Information					
Rank/GS Level/Contractor Job Title:					
Name (Last, First, MI):					
Complete Office Mailing Address:					
Government Employee or Uniformed Service Member Duty Station OR Contractor Sponsoring Organization Name: **(Not Project Name)**					
If Contractor, Employer Name:					
Is Applicant Working in Direct Support of the TRICARE Management Activity?	: □YES □NO				
Commercial Telephone Number:					
DSN:					
Email:					
IP Address of Workstation:					
Network Translated IP Address (if applicable)**:**					
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 EIDS WebPortal.**					

3. Action: Check Action Required: □NEW □CHANGE □DELETE □REACTIVATE

If you have a User ID, please enter it here: __________ (If your account has expired, enter your last USERID.)

4. Requestor Acknowledgement & Signature

Some data are protected under the provisions of the Privacy Act of 1974 and the DoD 6025.18-R and DoD 8580.02-R. The data contains patient and provider identity information and thus requires safeguards from unauthorized access and use. I agree to comply with applicable regulations 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 CDM for my current position/duty and agree to relinquish my CDM account to the EIDS Program Office 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."

User Signature____ **Date**__________________________

CDM – Clinical Data Mart
Account Authorization Request Form

5.a. Security Manager Certification of Background Investigation or Clearance Information
COMPLETE FOR ALL APPLICANTS

Type of Investigation	Date of Investigation (YYYYMMDD)	
Clearance Level	IT Level Designation □ Level I □ Level II	
Certified by (Printed Name)	Security Manager Phone ( )	Security Manager E-Mail Address

Security Manager Signature ____ **Date** ___________________

5.b. DUA Custodian Certification of Data Use Agreement (if required)

DUA Number		
Project Name on file with TMA Privacy Office		
Project Period of Performance		
DUA Custodian (Printed Name)	DUA Custodian Phone ( )	DUA Custodian E-Mail Address

DUA Custodian Signature ____ **Date** ___________________

5c. Use of Mobile Computing Equipment

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

□ Mobile computing equipment will not be used to connect to this EIDS product.

6. Commander, Supervisor or Security Officer Certification of Citizenship/Mission Need-to-Know
Complete this section for all applicants

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 CDM, and that the DUA referenced, if any, is applicable. I further acknowledge that substantial civil and criminal penalties 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) of 1996. 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 EIDS Program 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	
Email	
Office Mailing Address	
Commercial Telephone	
DSN	

Signature____ **Date**___________________

CDM – Clinical Data Mart
Account Authorization Request Form

7. Government Sponsor POC or Supervisor

All of the following information is required before a password will be assigned.

- If the user is a Government Employee or Uniformed Service Member, **Supervisor** must complete.
- If the user is a civilian contractor, **Government Sponsor point of contact** (POC) must complete.

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

I certify that the above named applicant requires access to CDM at the level I have indicated by my initials below. 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 POC/Supervisor Signature **Date**

8. CDM Roles with PHI – To be completed by Government Sponsor POC or Supervisor

The official duties of this individual require the following level of access (choose one):		Government Sponsor POC or Supervisor Initial Below ↓
MTF Patient Detail: User can create reports to view patient identifiable data within a specified MTF.		
MTF Name:	DMIS ID Family:	
Enterprise Data Miner Detail: User can create reports to view identifiable patient data for all patients across the health enterprise.		
Provider Detail: User is a provider and can create reports to view patient identifiable data for patients in his/her care**.**		
MTF Name:	DMIS ID Family:	

Applicant: Skip Blocks 9 & 10. Continue on Page 8.

9. EIDS Certification

□Form □SAC □WPValidPIN □AppSigned □CertSigned □SponSigned EIDS Access_____ □NTK____

I certify that EIDS requirements have been validated.
EIDS PO Approving Authority Name ____

Signature ____ **Date** ______________________

10. MHS TMA Privacy Office Access Approval Email Address dua.mail@tma.osd.mil

I certify that the applicant has □ has not □ met the requirements for ADP/IT security levels of trust; and

Has an approved DUA on file with the TMA Privacy Office □ YES □ NO □ N/A (Government & Military); and

Is a U.S. citizen (or has provided proof of U.S. Citizenship as required.) □ Is NOT a U.S. Citizen □

That the access level and justification is □ is not □ appropriate for their system use.

The Privacy Office approves □ does not approve □ the request for access to the MHS system.

Signature ____ **Date** ______________________

CDM – Clinical Data Mart
Account Authorization Request Form
DoD Minimum Security Requirements

The commercial Business Objects™ (BO) application used to support CDM, automatically communicates data to the user's PC in the process of building reports. Because this download may include sensitive data and the user does not control whether or not a download occurs, then the system to which the download is occurring must have at least the minimum security in place for protecting sensitive data. Under DoD and Service requirements, the local commander and appointed information system security officer are responsible for ensuring that automated systems under their control that store or process sensitive data meet minimum security standards. Normally, the process through which this is accomplished is a local certification/accreditation of the system at the DoD minimum-security requirement security level (as described in the DoD 8510.1-M;"DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual. Under legal and regulatory guidance, the EIDS PO, prior to allowing the transfer of sensitive data, must have assurance that the data will continue to be protected as prescribed by law and regulation. Thus, the requirement exists for a local commander or security officer to verify that any PC being used for sensitive data transfer is configured to meet minimum security requirements. **Contact your local network or System Security Officer for assistance with this certification.**

Some organizations do not have a process in place for obtaining local DoD minimum-security requirement level certification of a PC. In order to expedite the registration process, one of the following three statements, signed by your Organization Security Officer or Commanding Officer, will be accepted in order for you to obtain your account.

a. ____ The PC/Workstation assigned to ______________________ has been certified to be DoD minimum-security requirement compliant in accordance with DoD, Service, and local requirements; a copy of the certification or a statement by local Commander or Security Officer attesting to the **certification is attached**.

<u>or</u>

b. ____ The PC/Workstation assigned to ______________________ has removable media (**identify type of media**, i.e., Jaz Drive, CD-RW) that will be used for EIDS downloads; all such media will be protected in accordance with applicable requirements for handling and storage of sensitive data and marked accordingly (i.e., 'FOUO').

Specify type of media: ____

<u>or</u>

c. ____ The PC/Workstation assigned to ______________________, although not currently certified to be DoD minimum-security requirement level compliant, has been configured to meet as many of the DoD/Service mandated security requirements as feasible. Other mitigating actions (as listed below) are being taken to ensure that EIDS data is protected when downloaded**. I have reviewed the mitigating actions and accept the risk to sensitive data associated with the implementation of those actions.**

List mitigating actions taken: ____

____

[NOTE: For statement 'c' above, mitigating actions could be restricting physical access to the PC by placement in an office that is locked when not occupied, removal of the PC from network automatic logins, ensuring the PC is removed from network activity when not in use, and/or other measures deemed appropriate by local authorities.]

IA/ISO Signature ____**Date** ______________________

IA/ISO Printed Name ____

IA/ISO email Address ____**Phone (___)________________**

Clinical Data Mart – (CDM)
Account Authorization Request Form
Justification for Access to PHI

Generally speaking, only healthcare providers involved in the treatment of patients are allowed access to patient-identifying data regarding patients under their care. Such access could also extend to healthcare managers and administrative support personnel with specific, defined roles regarding paying or receiving reimbursement on medical claims and essential activities in support of health care operations. The use or disclosure of protected health information outside these parameters and without the patient's consent may violate the Privacy Act of 1974 and/or the Health Insurance Portability and Accountability Act of 1996 (HIPAA). A more detailed description regarding the required protection of individually identifiable data is available at http://www.usdoj.gov/04foia/privstat.htm and http://www.tricare.osd.mil/hipaa/.

Please identify your requirements for access to patient identifiable data. Please refer to Page 4 for guidance.

____

____

____

____

I acknowledge that:

1. Violations of the MHS Privacy Regulation are punishable by civil monetary penalties. In addition, a wrongful use or disclosure of protected health information is subject to criminal penalties. Offenses committed under false pretense or for commercial purpose also carry severe penalties.
2. I must not specify or retrieve any individually identifiable data in a CDM report unless such data is required to accomplish the mission of my organization.
3. I must maintain any patient-identifiable data in a fashion compliant with DoD minimum security requirements. Specifically, no individually identifiable data will be stored on a computer system or network or on media, which does not include both physical security against theft or access and password protection to access.
4. I must destroy all individually identifiable data as soon as it is not required for the organizational mission and keep a record of such destruction.
5. I must not retrieve any data based on unique individual identifiers from CDM and store such data locally for later retrieval UNLESS the retrieval is for a legal system of records, for which there is in place a separate agreement, approved by the TRICARE Management Activity, that the system can receive CDM data.
6. I must maintain a log, subject to audit, of any CDM data retrieval that I save where the data contains unique individual identifiers. The log will track any redistribution of the data to any destination or person, and the destruction of the data when it is no longer needed.
7. I cannot forward electronic copies of these reports with imbedded data to any other CDM user who does not have the same or higher level of access.
8. 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.

User Signature ____**Date** _______________________

Printed Name ____

Clinical Data Mart – (CDM)

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 Nil/DoD CIO memorandum, same subject, June 2, 2006, (c) DoD Policy Memorandum, “Department of Defense Guidance on Protecting Personally Identifiable Information (P11),” 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 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).

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 EIDS IAM, Mr. Curt Hefflin, Curtis.Hefflin.ctr@tma.osd.mil, or the EIDS IAO, Mr. Matt Aninzo, Materno.C.Aninzo@saic.com.

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

□ Laptop	□ External Hard Drive	□ CDs/DVDs	□ Floppy Disks
□ USB Flash/Thumb Drives	□ PDA	□ Cell Phone	□ Other

If other, please describe:
____

User 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 EIDS 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 EIDS product account is active.

User Signature ____**Date** ____________________

User Printed Name______________________________________

Information Assurance/Information Security 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 user’s computer. I will ensure that required updates are applied as available.

Make and model of mobile computing device(s):

Make	**Model**	**Serial Number**
________________	__________________	______________________
________________	__________________	______________________

IA/ISO Signature ____**Date** ____________________

IA/ISO Printed Name______________________________________

IA/ISO email Address _____________________________________**Phone** (___)________________