M2 – Military Health System (MHS) Management Analysis and Reporting Tool
Requirements for Receiving an M2 Account

For additional assistance, please call the DHA Global Service Center at 1-800-600-9332 (United States) or 1-866-637-8725 (Outside United States)

Account access to M2 is provided through the Solutions Delivery Division (SDD) Access Office. Due to the sensitive nature of the data contained within M2, several requirements must be met before users can obtain access to M2. The following describes what is needed to successfully be granted access to M2.

Required:

- ✓ All M2 users must have a valid Common Access Card (CAC) or Personal Identity Verification (PIV) Card
- ✓ The following documents must be emailed to SDD Access at dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil.
    - Signed and completed M2 Account Authorization Request Form
    - A copy of your DoD Information Assurance Awareness Certificate
    - A copy of your DoD Minimum Automated Information Systems (AIS) Requirements Certification/Compliance letter signed by your Information Assurance Manager or Information Security Officer
- ✓ To receive current e-mail notifications on M2 updates, news, and/or system outages, please register at https://public.govdelivery.com/accounts/USMHSDHSS/subscriber/topics

M2 – Military Health System (MHS) Management Analysis and Reporting Tool
Requirements for Receiving an M2 Account

For additional assistance, please call the DHA Global Service Center at 1-800-600-9332 (United States) or 1-866-637-8725 (Outside United States)

1. M2 Account Authorization Request Form (AARF)

The M2 AARF including Commanding Officer's/Government POC's certification of level of access *(Pages 5-11)* must be filled out, signed, and emailed to SDD Access Office at dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil. The SDD Access Office will grant access to M2. The following explains in detail all requirements needed to be completed in order to be granted access to M2.

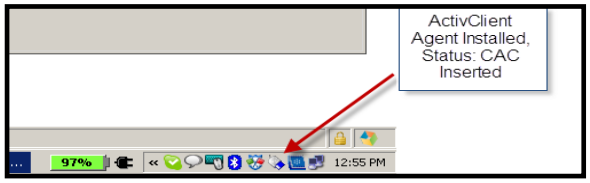
2. CAC/PIV Card Requirements

In order to access M2, each applicant must have a valid CAC or PIV card and your name and EDI PI must be entered on the M2 account access request form. To verify your CAC/PIV is valid please do the following:

PROCEDURE for Obtaining Information from Your CAC/PIV

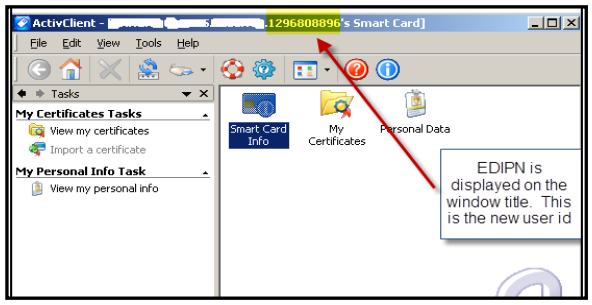
a) Verify CAC/PIV agent is installed, running, and that the CAC/PIV is inserted into the CAC/PIV reader.

b) Open the Information Panel. Right click on the CAC/PIV icon to access CAC/PIV information.



c) After you right click the icon, your Name and EDI PI is displayed in the window title.

   a. Enter this information in block 2 of the M2 account access request form.



3. DoD Information Assurance Awareness Training Certificate

DoD Directive 8570.01 *"Information Assurance Training, Certification, and Workforce Management,"* requires DoD information systems users each year complete Information Assurance Awareness Training. The SDD Access Office requires you submit a copy of your annual Information Assurance Awareness Certificate each year to SDD Access at via e-mail to dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil **.**

In order to continue to access M2 or any other SDD product, you must submit one copy of your signed DoD Information Assurance Awareness Certificate once a year to SDD Access via email to dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil .

<u>To access the annual DoD Information Assurance Training:</u>

1. Logon to http://iase.disa.mil/eta/index.html.
2. Select *Cyber Awareness Challenge* to take the training.
3. After successfully completing the training, print, or save, a copy of your Cyber Awareness Challenge Certificate.
4. Sign your certificate and send a copy to the SDD Access Office. Email the signed certificate to the SDD Access Office at dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil .
5. If you are outside the United States and have trouble submitting your certificate, please e-mail the DHA Global Service Center at servicecenter@dha.mil.

4. DoD minimum Automated Information System (AIS) Security Requirement Certified/Compliant Workstation and Encryption for Transmission of Restricted Data

DoD Directive 8500.01E, *"Information Assurance,"* states 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. Also, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) security rules, SDD requires an encrypted connection for transmission of Protected Health Information (PHI). Workstation encryption status for M2 will be determined during the M2 application process.

In order to certify adherence to DoD Directive 8500.01E, **a signed copy of your facility's DoD Minimum AIS Security Requirement Certification/Compliance letter** is required to be filed with SDD Access before access can be granted to M2. A signed copy of the DoD Minimum AIS Security Requirement Certification/Compliance letter can be e-mailed to dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil.

To get a signed copy of the Minimum AIS Security Requirement Certification/Compliance letter, M2 applicants should contact their local computer network or Systems Security Officer. For additional assistance please call the DHA Global Service Cente at 800-600-9332 (United States) or 866-637-8725 (Outside the United States).

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

Government and commercial vendors are required to provide data at rest encryption products for all mobile computing devices used to connect to SDD products. If an M2 applicant will be connecting to M2 using a mobile computing device, the M2 applicant is required to complete and submit a signed copy of the Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media on page 11.

Encryption Standards/Approved Software

- A Federal Information Processing Standards 140-2 approved file encryption algorithm (i.e., AES, 3DES) must be used for full disk encryption to encrypt data on any remote device that will be used to access M2. Mobile computing equipment users must also 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 approved data encryption products include but are not limited to:
  PGP Whole Disk Encryption – https://www.pgp.com/products/wholediskencryption/index.html
  GuardianEdge – http://www.guardianedge.com/products/guardianedge-hard-disk-encryption.php

DoD Components shall purchase data at rest encryption products through the DoD Enterprise Software Initiative (ESI), that substantially reduce the cost of common-use, commercial off-the-shelf software. For additional details, please log on to http://www.esi.mil or http://iase.disa.mil.

6. Requesting Appropriate M2 Level (Located on page 7, section 8)

SDD follows strict rules to verify patient identifiable data is provided only on a strict "need to know" basis. One safeguard are the requirements for M2 access authorization. For example, requests for M2 access to the restricted universe (patient names, social security numbers and/or pay grades) are closely and continuously monitored. To receive access to restricted data, clear and detailed written justification is required. This justification must include:

- Which patient identifiers, i.e., name, SSN and/or pay grades, are required.
- Why each required patient identifier is critical to perform the work or the organizational mission.
- The specific purpose and use of each patient identifier.

M2 uses query monitor software to capture all queries run against the reporting universes. All M2 accounts and queries run by those accounts are subject to constant electronic monitoring and analysis as well as random audits of use. ***If at any point it is discovered that the M2 database was queried for data not covered by the approved access justification; the account will be immediately suspended pending review.***

7. ADP-II/NACLC Clearance

Per DoD regulation 5200.2-R, non-DoD employees requesting access to M2 are required to have, or have submitted, a request for clearance, with a scheduled Investigation Scheduled Notice 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.

8. Data Sharing Agreement

To confirm that the data will be used in compliance with the applicable privacy requirements, contractors and non-government employees who seek to obtain PHI/Personally Identifiable Information (PII) via M2 access, to perform a government-sponsored initiative, and government personnel (civilian and uniformed service members) requesting M2 access to conduct research, are required to have a current Data Sharing Agreement (DSA) on file with the Defense Health Agency (DHA) Privacy and Civil Liberties Office (Privacy Office). If you do not have an active DSA, please contact the Privacy Office at dha.ncr.health-it.mbx.dsa-mail@mail.mil.

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form (AARF)

1. 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 (Applicant must describe)

2. Applicant/Requestor Information	
Rank/GS Level/Title:	
Name (Last, First, MI) from CAC or PIV:	
Office Mailing Address:	
Sponsoring Organization Name/Active Duty or Civil Service Duty Station: **(Not Project Name)**	
If Contractor, Employer Name:	
Commercial Telephone Number:	
Email:	
IP Address of Workstation: (if applicable)**:**	
Applicant's EDI PI number from CAC or PIV:	
Account Validation PIN: Enter a 4 digit numeric PIN that you will use to validate your identity for account administration purposes.	

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

4. Requestor Acknowledgement & Signature

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 as implemented within DoD 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*. If granted access to restricted data, I will not attempt to use the access for any purpose except as required for official duties.* I understand that my access may be revoked or terminated for non-compliance with DoD security policies including completion of annual Privacy and HIPAA training. 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 M2 for my current position/duty and agree to relinquish my M2 account to the SDD Access 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."***

Applicant Signature_____ **Date**_____

CONTINUED ON NEXT PAGE

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form (AARF)

5. 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.
Certification is on the last page and **MUST BE COMPLETED.**

☐ Mobile computing equipment **will not be used** to connect to this SDD product.

6. Commander, Government POC or Security Officer Certification of Citizenship/Mission Need to Know Acknowledgement

By signing below, I am certifying that _____ (applicant) is a U.S. Citizen and has a mission essential or contract-driven requirement to access M2, and that the Data Sharing Agreement 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 HIPPA. I will report any change in status, duties, position, or location of the applicant that indicate that the access granted is no longer required. ***I agree to notify the SDD Access Office upon departure of this applicant from their current position/duty or when access is no longer required.***

Commander/Government POC/Security Officer Name	
Title or Position	
Organization, Office, Company	
Email	
Mailing Address	
Office Telephone	
DSN	

Signature_____ **Date**_____

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

- If the applicant is an active duty military or civil service employee, Government POC must complete.
- If the applicant is a civilian contractor, Government POC must complete.

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

I certify that the above named applicant requires access to M2 at the level I have indicated by my initials In blocks 8 and 8a (if appropriate), 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 POC Signature **Date**

CONTINUED ON NEXT PAGE

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form (AARF)

8. Level of Access – To be completed by Government POC	
The official duties of this individual require the following level of access (select one of the following):	Government POC Signature Below ↓
Reporter*: User can create reports against all tables (summary & detail) for all Military Treatment Facilities and corresponding DMIS ID's, but can only view pseudo-patient identifying data. Users can create reports, refresh reports, and save to personal folders.	
Publisher*: User can create and publish reports against all tables (summary & detail) for all Military Treatment Facilities and corresponding DMIS ID's, but can only view scrambled patient identifying data. Users can create reports, refresh reports, and save to Public Folders in addition to personal folders. ***Note: New users will not be authorized to receive this access level. This access will require approval from M2 Functional Sponsor and Service Representative.***	
*Requires Government POC signature on the previous page.	

8A. Protected Health Information Access	
The official duties of this individual require access to patient identifying data. This section should only be completed IF the User requires access to restricted data.	Government POC Signature Below ↓ (Same POC signature is required on page 10 to approve this permission level)
Restricted **: User requires access to patient identifying data for all Military Treatment Facilities and corresponding DMIS ID's. It is essential that the user have a thorough knowledge of Privacy Act and HIPAA rules, restrictions and the proper security clearance. Restricted data Access is required in addition to either the Reporter or Publisher Level of Access specified above.	
Requires Unit Commander (or equivalent, or by direction) signature on the previous page and completion of the **Justification Form *(page 9)*.	

Applicant: Make No Mark Below. Requests for Restricted Data Access and Contractors go to pages 8, 9 & 10.

9. SDD Access Office Certification

☐Form ☐DoD IA ☐WPValidPIN ☐AppSigned ☐CertSigned ☐SponSigned SDD Access_____

I certify that SDD requirements have been validated.
SDD PEO Approving Authority Name _____

Signature _____ **Date** _____

10. Encryption for Restricted Accounts – SDD Use Only

☐ **The workstation identified in this application has been certified as having an encrypted connection capability for transmission of restricted data. The workstation was certified on (date):** _____
by (name): _____ **through:**
☐**DISA – Netscreen or other device** ☐**SDD provided Checkpoint VPN SecuRemote**

☐ **Other approved method (specify):** _____

☐ **This workstation was not capable of meeting encryption requirements. Applicant was denied access to restricted data.**

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form (AARF)

DoD Minimum Automated Information System (AIS) Security Requirements

The commercial Business Objects™ application used in M2 may automatically download data to a user's workstation in the process of building reports. Because this download may include sensitive data and a user does not control whether or not a download occurs, then the system to which the M2 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. Under legal and regulatory guidance, SDD requires written assurance from a local commander and/or security officer before allowing the transfer of sensitive data to M2. ***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 personal computer. In order to expedite the M2 registration process, one of the following three statements signed by your organization's Security Officer or Commanding Officer will be accepted in order for you to obtain an M2 account.

a. ____ The 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**.

OR

b. ____ The Workstation assigned to _____ has removable media (**identify type of media**, i.e., Jaz Drive, CD-RW) that will be used for M2 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: _____

OR

c. ____ The 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 M2 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: _____

_____

(Mitigating actions can be restricting physical access to the workstation by placement in an office that is locked when not occupied; removal of the workstation from network automatic logins; ensuring the workstation is removed from network activity when not in use; and/or other measures deemed appropriate by local authorities.)

Information Assurance Manager/Information Security Officer Signature

_____**Date**_____

IAM/ISO Printed Name _____

IAM/ISO email Address _____**Phone**_____

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form Justification for Access to Restricted Data

Access to Restricted Data

Generally speaking, only healthcare providers involved in the treatment of patients are allowed access to restricted (patient-identifying and protected health information) 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 restricted data outside these parameters and without a patient's consent may violate the Privacy Act of 1974 and/or HIPAA. For additional DoD guidance regarding these federal privacy laws, please go to http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties.

Please lists your requirements for access to patient identifiable data in M2.

_____

_____

_____

_____

I acknowledge that:

1. *Violations of HIPAA may result in significant disciplinary action. In addition, a knowing wrongful use or disclosure of protected health information is subject to criminal penalties of up to a $50,000 fine and one year imprisonment. Offenses committed under false pretense or for commercial purpose carry more severe penalties.*
2. *I must not specify or retrieve any individually identifiable data in an M2 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 the "DoD minimum security requirements" stated on the preceding page.*
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 M2 and for transfer (e.g. by storage of such data locally) to a separate Privacy Act system of records, unless there is in place a separate agreement, approved by the Defense Health Agency, authorizing that system to receive M2 data.*
6. *I must maintain a log, subject to audit, of any M2 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 M2 data to any other M2 user who does not have the same or higher level of access.*
8. *I understand and accept that my use of the M2 system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems.*

Applicant Signature _____**Date** _____

Printed Name _____

M2 – MHS Management Analysis and Reporting Tool
Account Authorization Request Form Justification for Access to Restricted Data

GOVERNMENT POC ACKNOWLEDGEMENT OF PHI RESPONSIBILITY

I certify that (sponsored applicant) _____ will abide by the guidelines listed below and requires access to this data for the reasons identified in the M2 request.

I am aware that it is a shared responsibility between everyone to protect PHI and Privacy Act data from misuse. By affirming to the above statement, I am confirming the following:

- *I have direct supervision over the user and can confirm this user requires access to PHI in order to perform his/her job.*
- *The user's workstation meets the DoD Minimum Security Requirements.*
- *PHI and Privacy Act data will be safeguarded within my facility.*
- *I will notify SDD Access when the user no longer requires access to PHI or when he/she has changed locations.*

GOVERNMENT POC'S SIGNATURE_____ DATE _____

PRINTED NAME_____

M2 – MHS Management Analysis and Reporting Tool
Contractor and Research Requirements Security Clearance/ADP and Data Sharing Agreement

1. Non-DoD employees: ADP-II Clearance

Per DoD regulation 5200.2-R (Appendix 10 of the Personnel Security Program), non-DoD employees requesting access to M2 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) clearance.

2. Data Sharing Agreement (DSA) r**equirements**:

The DHA Privacy and Civil Liberties Office (Privacy Office) uses a DSA as an administrative control measure to verify that contractors and non-government personnel (using the PHI/PII for purposes other than patient care) and for government personnel (using the data for research purposes) will use and safeguard DHA data in compliance with applicable privacy requirements.

Requesting individuals indicated above, requiring access as Reporter or Publisher for M2 data, are required to have a current DSA on file with the Privacy Office.

For information pertaining to Data Sharing Agreements, please refer to the TMA DHA Privacy and Civil Liberties Office website at http://www.tricare.mil/tma/privacy/ or contact them via email at dsa.mail@dha.mil.

3. Non-DoD employees: Additional M2 Account Authorization Request Form Information

In accordance with the DHA Privacy Office, the below information must be completed and submitted to the SDD Access Office along with the M2 Account Authorization Request Form.

Please complete and submit with M2 AARF (pages 5 - 11) to the SDD Access Office via email at mailto:dha.ncr.dhss-prog-sup.mbx.dhss-access@mail.mil. If you are outside the United States and are having trouble, please contact the DHA Global Service Center at servicecenter@dha.mil for an alternate number.

MHS Contractors, Researchers, or other Non-MHS Employees, MUST provide the following information:

Employer Name: (i.e. DoD)	
US Citizen:	☐ **YES** ☐ **NO**
Complete Contract Company Mailing Address:	
Name and Phone Number of Security Lead **Contract Company Email Address:**	
Project Description requiring this Access:	
What is the DSA # or Project name on file with the DHA Privacy and Civil Liberties Office?	
Project Period of Performance:	
Applicant Security Level (mark appropriate level): **ADP Level I** ☐ **ADP Level II/NACLC** ☐ **Other (specify)** _____	
If access based on SECRET clearance provide applicant Date and Place of Birth:	

DSA Applicant/Recipient Signature_____ **Date**_____

M2 – MHS Management Analysis and Reporting Tool
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, 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 SDD IAM, Mr. Nick Saund: Narinder.S.Saund.civ@mail.mil or 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 restricted data from this SDD product: (check all that apply). Use of USB THUMB DRIVES is PROHIBITED BY DoD REGULATION.

☐ 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, restricted data) 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/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 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/ISO Signature _____**Date** _____

IAM/ISO Printed Name_____

IAM/ISO email Address _____**Phone**_____