IMD - INPROCESSING PACKET PROCEDURES

1. Information management in-processing requirements are established by DoD, Army, and MEDCOM, and are not negotiable. **If you are a Healthcare Provider, it is best to begin with the Credentialing department so that process is expedited.**

   a. IMD hours for In- and Out-Processing are 0900-1100 & 1300-1500, M-T-W-F

   b. Mailroom: 1230-1430 at the mailroom, or 0730 - 1630 M-F at PAC, in the Medical Company in Bldg 248-A

2. Instructions for *NTC-657-2-E,* User Access Request and Responsibility Statement:

Part II - Complete with information about yourself. **(Areas 1-10 must be completely filled out)**
Part III - Completed by the Security Manager, PTM&S, Building 174 **(see paragraph 5).**
Part IV - 1 - Complete and sign.
Part IV - 2 - Take to your supervisor for completion.

3. *Fort Irwin MEDDAC Acceptable Use Policy & DOD Information System User Agreement* - Please read the entire document carefully. There are two copies of the signature page (Page 18) in the packet. Keep one copy for yourself, print your name and rank, sign and date the other copy of the signature page (Page 19) for our records.

4. You must provide IMD evidence of training in *DOD IA Awareness (INFOSEC), Army G3 Computer Security Training, Personally Identifiable Information (PII), Safe Home Computing, Phishing Awareness, Portable Electronic Devices and Removable Storage Media* and *HIPAA.* All training links and information is located in the following locations:

   a. **Intranet -** (http://amedapwach106). Then click on the 'Training' link located on the top menu bar.
   b. **Internet -** (http:l/www.irwin.amedd.army.mil). Under 'Classes at MEDDAC', click on 'MEDDAC Personnel In-processing Information' link located on the lower right.

5. Take the *NTC-657-2,* Fort *Irwin MEDDAC Acceptable Use Policy,* and *DOD IA Awareness (INFOSEC)* training certificate to PTM&S in building 174 for completion of the security manager portion (Part III) of the NTC-657-2.

6. No accounts will be created until all of the above training / documents are filled out andlor printed and returned to IMD in building 166, room 110. **(Reference the "Return to IMD -- Checklist")**

7. Login Procedures Document - Keep for reference when logging onto the LAN, AHLTA, and CHCS after accounts are created. **If you need an AHLTA, CHCS or Essentris account, your department must complete a CHCS/AHLTA and Essentris User Access Request Form *for* you to bring to IMD, stating the keys and menus you need to have assigned to you.**

Return to IMD Checklist

Name:_______________________________________

NTC-657-2 _____

Fort Irwin MEDDAC Acceptable Use Policy &
DOD Information System User Agreement _____

DOD IA Awareness (INFOSEC) _____

Confirm HIPAA Training completed
(Print Transcript) _____

Army G3 Computer Security Training
Certificate _____

Personally Identifiable Information (PII) _____

Safe Home Computing Course _____

Phishing Awareness Course _____

Portable Electronic Devices and Removable
Storage Media Course _____

CHCS/AHLTA User Access form **(if needed)** _____

Essentris User Access form **(if needed)** _____

GETTING STARTED WITH MHS LEARN

(HIPAA) TRAINING

AT FORT IRWIN

This guide will lead you through the registration process to begin your MHS Learn HIPAA Training.

Hours for HIPAA Training: 0800-1100 M-F, IMD Training Room, Bldg 174

New Users
New users to the MHS Learn application must complete the self-registration process. The student ID will be system generated and you will create your own password. You must enter your student ID and password to re-visit the MHS Learn Training website.

All Users:
Upon completion, you must print out your Transcripts. To access your transcripts you must log –in, click on the "profile" tab in the upper right corner, click on the transcripts tab in the upper left corner.

If you encounter any problems, please contact Mr. Carlos Garcia at DSN 470-6889 or com: 380-6889.

1. Getting Started
Access the MHS Learn Training application by visiting: https://mhslearn.satx.disa.mil

2. MEDDAC, DENTAC, and YUMA in processing personnel
Once you locate your Domain, highlight it in the drop down list, then scroll to the bottom of the screen and click ok.

<u>Domains:</u>
MTF/Location/Unit is: ARMY - 11 Western – WEED ACH (0131)
MTF/Location/Unit is: ARMY - 11 Western – YUMA (0206)
MTF/Location/Unit is: ARMY - 11 Western – DENTAC ACH (6032)

3. Password
The password must meet DOD password criteria. If you have already **Self Registered** once, **DO NOT** attempt Self Registration again. Click Cancel and login with your user name and password. User name format is **FirstName.LastName.1234** (your last four SSN). If you forgot your password go back and click Forgot Password link.

USER ACCESS REQUEST AND RESPONSIBILITY STATEMENT

For use of this form, see AR 25-2

Privacy Act Statement

AUTHORITY:	10 U.S.C. 3013
PURPOSE:	To control access, through password and user identification codes, to Government Information Systems.
ROUTINE USE:	To identify data processing and communications customers authorized access to Government Information Systems.
DISCLOSURE:	Voluntary; however, failure to provide information may result in denial of access to automation systems.

PART I - ACTION REQUESTED

1. Type of action □ a. New Account □ b. Delete Account □ c. Change	2. Login ID affected (*If action is other than a new account*):

3. Access Requested on the following systems (Check all that apply):

□ a. Logon Only □ b. Exchange □ c. Official Mailbox: ____________________

□ d. TSACS □ e. SIPRNET □ f. Distribution List: ____________________

PART II - REQUESTOR INFORMATION

1. Name *(Last, First, MI)*		2. Grade/Rank: □ Military □ Civilian □ Contractor	3. Social Security Number last 4
4. Organization/Position:	5. Office Symbol:	6. Building/Room Number:	7. Duty Telephone Number:
8. AKO Address: @us.army.mil		9. Security CD Training Date:	10. Date on Acceptable Policy:

PART III - SECURITY ACCESS VERIFICATION

1. Information Technology (IT) Position: □ IT - III □ IT - II □ IT - I		2. Security Investigation: □ ENTNAC □ NAC □ NACI □ SSBI		
3. Date Investigation Submitted:	4. Investigation Date:	5. Access to Classified System □ YES □ NO	6. Clearance Level:	7. Date of Clearance:

8. Activity/Unit Security Manager or Facility Security Officer: I verify user has proper security investigation/clearance for system.

a. Print/Type Name:	b. Signature:	c. Date:

PART IV - RESPONSIBILITIES REQUIREMENTS

As a potential user of Government information systems resources, I am aware of the following responsibilities: I will use the resources only in the performance of my official duties. I will control and protect all data, software, hardware, and passwords and copyrighted or proprietary material to the best of my abilities. I will not use personally owned computers to access Government information system resources. I will immediately report suspected security incidents to my IASO. I will protect my user account name and password, and telephone access numbers at a level commensurate with the level of information being processed or accessed. I will abide by applicable security regulations and guidelines, and access only the resources authorized. I understand the password I use as a result of this request is my personal access key and if I reveal my password to anyone, the password will be considered compromised and my access privilege suspended or revoked pending an investigation of the compromise.

1. REQUESTER: I have read the above and will comply to the best of my ability.

a. Print/Type Name:	b. Signature:	c. Date:	d. Duty Phone:

2. SUPERVISOR: I verify this access request is authorized.

a. Print/Type Name:	b. Signature:	c. Date:	d. Duty Phone:

3. CONTRACTING OFFICER: I certify this request and authorization is required under the scope of the existing contract.

a. Print/Type Name:	b. Signature:	c. Date:	d. Duty Phone:
e. Print/Type AKO Sponsor's Name:	f. Signature	c. Date Contract/access expires (***required entry***):	

4. IASO/AO: I verify user has proper security clearance/investigation, understands security guidelines, and is an authorized user.

a. Print/Type Name:	b. Signature:	c. Date:	d. Duty Phone:

Instructions

Part I

1. Type of action. Indicate what type action you want to be taken.
2. Login ID affected. Use this if you are making a change to an existing account.
3. Access Requested. Check all that apply.

Part II

1. Name. Please give your full name. If you wish to use a shortened version of your name such as Joe instead of Joseph write it in the blank space (margin) in the upper right corner of the form.
2. Grade or Rank.
3. Social Security Number. Last 4 only
4. Organization.
5. Office Symbol: This must be a valid Office Symbol IAW NTC Supplement 25-1.
6. Building/Room Number.
7. Duty Telephone Number.

Part III

1. IT Position.
2. Type of Security Investigation.
3. Date investigation submitted.
4. Investigation Date.
5. Access to Classified. If no, skip 6, & 7.
6. Clearance Level.
7. Date of Clearance.
8. Activity/Unit Security Manager or Facility Security Officer.

Part IV

1. Requestor.
2. Supervisor.
3. Contracting Officer. If the requestor is a contractor, the Contracting Officer must sign block 3 of Part IV and provide an expiration date. Indefinite or unknown is NOT acceptable.
4. IASO or AO.

SUBMISSION PROCESS

Final signature and reviewer is the Information Assurance Security Officer (IASO). The IASO is responsible for ensuring all responses are provided and follow-up on requests submitted with an ADP Waiver. Once the IASO accepts the request they are responsible for maintaining the completed original, sending a copy to the IAM, attaching a copy to the accreditation package, and submitting the request to the DOIM Postmaster via email. The DOIM Postmaster will establish accounts submitted by the IAM, IASO or AO only. This authority may be delegated to an alternate IASO or the IMO; however, this delegation must be made in writing and submitted to the IAM. The IAM will maintain a list of personnel authorized to establish accounts which can be viewed in the DOIM Public Folders, under Information Assurance.

APPENDIX A
ACCEPTABLE USE POLICY (AUP)

1. Understanding. You have the primary responsibility to safeguard the information contained in USA MEDDAC, Ft. Irwin information systems (IS) from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

2. Access. Access to the USA MEDDAC IS is for official use and authorized purposes and as set forth in DoD 5500.7-R, Joint Ethics Regulation, or as further limited by this policy.

3. Revocability. Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified Information Processing. USA MEDDAC IS are not authorized to process any level of classified information.

5. Unclassified Information Processing. USA MEDDAC IS are the primary unclassified automated administration tools for USA MEDDAC. The USA MEDDAC IS are US-only systems.

a. USA MEDDAC IS provide unclassified communication to external DoD and other United States Government organizations.

b. USA MEDDAC IS are approved to process UNCLASSIFIED, SENSITIVE information in accordance with AR 25-2, Information Assurance.

c. USA MEDDAC IS and the Internet, as viewed by USA MEDDAC, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the NIPRNET and Internet.

6. Minimum Security Rules and Requirements. As a USA MEDDAC IS user, the following minimum security rules and requirements apply:

a. Personnel are not permitted access to USA MEDDAC IS unless in complete compliance with Department of the Army personnel security requirements for operating in a system-high UNCLASSIFIED SENSITIVE environment (AR 25-2, Section V, Personnel Security).

b. Personnel will complete initial security awareness training before being granted system access. Personnel will complete yearly refresher training as required by AR 25-2 and other yearly and one-time training as required by Department of the Army and USA MEDDAC policy. Access to the USA MEDDAC IS may be revoked if required training is not completed.

c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not create passwords using my user name, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words.

d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized classification level.

g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the USA MEDDAC IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize Army- or DoD-provided IS for commercial financial gain or illegal activities.

k. Maintenance will be performed by the System Administrator (SA) or Help Desk Technicians only.

l. I will use screen locks or log off the workstation when departing the area. I will restart my workstation at least once a week.

m. I will immediately report any suspicious output, files, shortcuts, or system problems to the IMD Help Desk, and /or Information Assurance Security Officer and cease all activities on the system. The IMD Help Desk may be reached at 380-6291. The Information Assurance Security Officer may be reached at 380-1373.

n. I will address any questions regarding policy, responsibilities, and duties to the IMD Help Desk, and /or the Information Assurance Security Officer.

o. I understand that each workstation is the property of the Army and is provided to me for official and authorized uses. I further understand that each workstation is subject to monitoring for security purposes and to ensure that use is authorized. I understand that monitoring of USA MEDDAC IS will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that I do not have a recognized expectation of privacy in official data on the USA MEDDAC IS and may have only limited expectation of privacy in personal data on the USA MEDDAC IS. I realize that I should not store data on the USA MEDDAC IS I do not want others to see.

p. I understand that as part of the security process, members of the Information Assurance or HIPAA staff may occasionally inspect my area to ensure that I have locked or logged off my computer when I am away, that I do not have passwords posted in an easily accessible place, and that I am in compliance with other information assurance and HIPAA security policies.

q. I understand that social engineering techniques are sometimes used to attempt to get users to give up their password. I will NEVER give my password to anyone, including administrators and persons claiming to be IMD Help Desk personnel. If this happens, I will report it to the IMD Help Desk immediately.

r. I understand that the following activities define unacceptable uses of an Army IS :

(1) Viewing web sites with pornographic, extremist, anti-U.S. Government or anti-U.S. military content or any other content prohibited by DoD Regulation 5500.7-R or my supervisor.

(2) Using USA MEDDAC-provided workstations for private, commercial or political activities.

(3) Sending or replying to mass e-mails (i.e., chain letters, spam, etc.).

(4) Sharing account information such as passwords or allowing other staff members to use someone else's account.

(5) Viewing patient or administrative data without a specific need to know.

(6) Transmitting patient or administrative data to someone that lacks a specific need to know.

(7) Accessing commercial e-mail or instant messaging sites/applications (Hotmail, AOL or Yahoo mail, MSN or AOL messenger, etc.).

(8) Using Army IS to perform actions specifically denied or restricted by the immediate chain of command, (i.e., first line supervisor, NCOIC, etc.), this policy, MEDCOM policy, U.S. Army regulations or applicable State and Federal Laws.

(9) Engaging in any activity that could reasonably be expected to cause, directly or indirectly, congestion, delay or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications. Such uses include, but are not limited to, the use of communications systems to:

(a) Create, download, store, copy, transmit, or broadcast chain letters

(b) "Spam" to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail

(c) I will limit the sending of messages to the minimum number of personnel. If I have information that needs to go out to a large number or all of the USA MEDDAC, DENTAC and/or YHC, I will send it to the MEDDAC Newsletter for publication on Tuesdays and Fridays.

(d) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with their use of e-mail.

(e) Broadcast unsubstantiated virus warnings from sources other than systems administrators.

(f) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations

(g) Employ for personal use applications using streaming data, audio, and video; malicious logic and virus development software, tools, files; unlicensed software; games; Web altering tools/software; or any other software that may cause harm to Government computers and telecommunications systems.

s. I understand that the Internet, email, telephone, cell phones, and blackberries are

(1) Provided for performing official duties. This includes career development and training, if approved by my supervisor. Use of the Internet, email, cell phones, blackberries, and long-distance PIN number for telephone calls is a privilege that may be revoked at any time for inappropriate use or misconduct. Official use of the Internet, email, cell phones, blackberries, and long-distance PIN number for telephone calls is defined as that which is necessary in the interest of the Government (directly related to conducting our business). There are a few exceptions to the “official use” rule. I understand that I may make infrequent, short personal communications and Internet searches, provided that they:

(a) Do not adversely affect my performance of official duties.

(b) Are of short duration and infrequent, and made during my personal time such as breaks and lunch.

(c) Do not adversely reflect on the MEDDAC, the Army or the Department of Defense.

(d) Are not used for activities related to the operation of a personal business.

(e) Are of no additional cost to the Government. I understand, therefore, that I may not use my MEDDAC-issued long distance PIN number to make anything other than official calls. If I do, the Commander is obligated to recoup these charges from me and I may be subject to administrative or disciplinary action. Official calls are those calls directly related to the performance of my duties. If I need to make a personal long distance toll call while at work, it must be: charged to my home number, made to a toll-free number, a collect call, or charged to my personal credit card or telephone calling card.

(2) Cell phones, radios, cameras, video cameras, and camera phones are not to be used in the hospital without written permission from the Safety Manager or HIPAA Privacy Officer. The Safety Manager must approve use of any cell phones and radios before they can be operated since they have the potential to interfere with electronic medical equipment. The Privacy Officer must approve all camera devices due to a significant privacy concern when

taking pictures in patient care areas. Even “official” devices, such as Government-owned cameras and equipment, must be cleared before use. I will help enforce this policy by ensuring that patients and visitors understand it. If a visitor does not follow my instructions regarding this, I will report it to my supervisor right away. Likewise, media members are not to be allowed to take pictures or make notes regarding activities in the hospital unless they have been cleared and they are escorted by the Public Affairs Officer from IMD and/or a member of the Governing Board. If I see unescorted media personnel, I will report it to my supervisor and I will call the IMD Help Desk at 380-6291.

(3) All email and faxes containing Privacy Act information or ePHI must also contain the following confidentiality notice: “This document may contain information covered under the Privacy Act, 5 USC 552(a) and/or the Health Insurance Portability and Accountability Act (PL104-191) and its various implementing regulations and must be protected in accordance with those provisions. Health care information is personal and sensitive and must be treated accordingly. If this correspondence contains health care information, it is being provided to you after appropriate authorization from the patient or under circumstances that do not require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure, and confidential manner. Re-disclosure without additional patient consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality subjects you to application of appropriate sanctions. If you have received this correspondence in error, notify the sender at once and destroy any copies you have made.”

t. I understand that each USA MEDDAC IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each USA MEDDAC IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the USA MEDDAC IS and may have only a limited expectation of privacy in personal data on the USA MEDDAC IS. I realize that 1 should not store data on the IS that I do not want others to see.

u. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary; however, failure to disclose information could result in denial of access to USA MEDDAC IS.

7. Use of Digital Signature and Encryption in Email.

a. I understand that a digital signature is not required on email messages, but may be used as follows:

(1) To verify the identity of the sender of a message.

(2) When non-repudiation is required. Non-repudiation means that the sender cannot later deny having sent the message.

b. I understand that encryption is required on all email sent between MEDCOM users that contains Privacy Act information, sensitive information, or EPHI sent between MEDCOM users. When in doubt, I will encrypt.

c. If I am a provider communicating by email with a patient, and I know the patient has encryption capability (such as when the patient is a MEDDAC employee), I will encrypt all provider-to-patient communication with him/her.

d. Both digital signature and encryption can be used within Microsoft Outlook. Once I have a Common Access Card (CAC, the ID card with the chip in it), a CAC reader installed on the PC I use, and the feature set up within my Outlook email, I will be able to digitally sign, encrypt or decrypt messages. I will test this feature after my email account has been set up, and if it is not working or I need help, I will call the IMD Help Desk.

e. I also understand that encryption does not prevent me from sending email to the wrong user. If I accidentally select the wrong user from the Global Address List (GAL), and encrypt the message, that person will be able to decrypt and read it. Therefore, I must use caution when picking names out of the GAL.

8. Mobile Computing Devices. If issued or using a mobile computer to include laptop, notebook, tablet or other mobile computing device, I will comply with the following requirements:

a. I agree to bring my laptop, tablet PC, or other mobile devices to the USA MEDDAC and connect them to the LAN monthly at a minimum to allow for regular security scanning, virus updates, and security patching. The only exceptions are for persons on temporary duty or deployed status.

b. If my equipment is on temporary loan from IMD, I will return it to IMD within three business days after using it or upon returning from my trip.

c. I will store the laptop or other mobile computing device in a locking container or secure it with a locking cable to my desk if it remains in my office or work space.

d. I will properly secure the laptop and other mobile computing device(s) at all times. I will never leave it unattended in my car, conference room or hotel room for any reason.

9. Remote Access. I understand remote access to the USA MEDDAC virtual private network (VPN) is for official use by the designated user only. All policies and regulations that apply to use within USA MEDDAC apply to remote access.

10. Wireless Network Access. I understand wireless network access to the USA MEDDAC LAN is for official use by the designated user only. All policies that apply to use within USA MEDDAC apply to wireless network access. Wireless access to the USA MEDDAC is approved for government owned computing devices only.

11. Violations: Violations of this policy can result in revocation of the authorization to use the network, systems, PIN numbers, telephones or all of these. The violator may be subject to administrative, civil or non-judicial action. The type of sanction applied varies, depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors. As a rule, USA MEDDAC's sanctions consist of:

a. First Violation:

(1) The IMD notifies the offender and his or her immediate supervisor in writing of the policy violation and provides a copy of this Acceptable Use Policy statement, acknowledged and signed by the user, highlighting the appropriate sections. MEDDAC 25-2 or AR 25-2 may also be cited as necessary.

(2) Depending on the severity of the violation, the user may have his/her access revoked until retraining is completed. Retraining may consist of Computer Users Security Training, additional HIPAA training, or review of this policy.

b. Second Violation:

(1) The user's computer, network and systems access will be revoked immediately.

(2) The IMD notifies the offender and his or her immediate supervisor in writing of the violation, and provides a copy of this Acceptable Use Policy statement. The IASO will also notify the user's Deputy Commander or Command Sergeant Major of the violation. Until the Deputy Commander or Command Sergeant Major notify IMD that the offender has been sanctioned, punished or admonished appropriately, the user will not regain access to accounts.

(3) The supervisor counsels the offender regarding the violation of information security regulations in writing and provides a copy of the counseling to the IASO and HSO. The offender must re-read and re-sign the MEDDAC acceptable use policy and successfully re-complete Computer User's Security Training and HIPAA security.

(4) The IMD restores access when all actions are complete.

c. Third Violation:

(1) The user's access to all systems is revoked immediately. The IASO will notify the Security Manager that the individual has displayed a pattern of continued disregard for written policies.

(2) The IMD notifies the offender and his or her immediate supervisor in writing of the violation, and provides a copy of this Acceptable Use Policy statement. The IMD will also notify the Deputy Commander or Command Sergeant Major of the violation.

(3) Due to increased risk, the USA MEDDAC Commander is the only one who can authorize the individual's continued access to any and all information systems.

(4) The IASO either restores or deletes all of the user's accounts, based upon the Commander's decision.

d. For all violations, the HIPAA Security Officer will investigate the violation and determine whether it was also a HIPAA violation. If so, the CIO will notify the Governing Board and make a recommendation regarding whether to pursue additional administrative, civil or legal actions relating to HIPAA security violations. This is based upon the nature and scope of the violation as well as past conduct.

12. STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

- You consent to the following conditions:

  - The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

  - At any time, the U.S. Government may inspect and seize data stored on this information system.

  - Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

  - This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

  - Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

      - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

13. Acknowledgement. (User copy)

I have read the above requirements regarding the use of the USA MEDDAC IS. I understand my responsibilities regarding these systems and the information contained in them.

Directorate/Division/Branch

Date

Last Name, First, MI

Rank/Grade/SSN

Signature

Phone Number

- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

13. Acknowledgement. (IMD copy)

I have read the above requirements regarding the use of the USA MEDDAC IS. I understand my responsibilities regarding these systems and the information contained in them.

____________________________ ________________________________
Directorate/Division/Branch Date

____________________________ ________________________________
Last Name, First, MI Rank/Grade/SSN

____________________________ ________________________________
Signature Phone Number

LOGIN PROCEDURES

ADMIN LAN

Common Access Cards (CAC) are now used for accessing Government computers. Military personnel, your CAC is your ID card. Civilians and Contractors must obtain a CAC card as part of their in-processing. You will not be able to use your CAC to logon until your account has been created.

AMED accounts are normally created within 3 business days of the completed paperwork being submitted to IMD. After that period, you should be able to login to any computer in your department by inserting your CAC into the reader and typing in your 6-8 digit all numerical PIN that you created when you obtained your CAC. Contact IMD after the 3 business day period if you can not log in.

EXCHANGE MAIL (Outlook)

Once you are logged into the LAN (above), you will need to contact IMD via a HEAT Ticket (located at the home page of the Intranet) or call IMD @ **4-6291** to have your Outlook mail profile set up on the PC you will be using. 4-6291 is an answering machine, so please leave your name and a good call back number so we may get back to you as soon as possible to set up your profile. There is also an IMD Self Help link on the home page of the intranet (just open up Internet explorer and hit "yes" on the dialog box) that has step by step instructions on how to set up your outlook.

Your email address is your AKO user name with "@us.army.mil" at the end.

CHCS/AHLTA

If an AHLTA request form was submitted with your IMD In-Processing packet, please be patient as it could take up to a week to create your AHLTA account. Once your account has been created, IMD will send you an e-mail or contact you by phone to let you that your account is completed and provide you with your username and password. If AHLTA is mission critical, let us know and we will attempt to expedite this proces