

ELECTRONIC HEALTH RECORD APPLICATION - USER REGISTRATION

*** PRIVACY ACT 1974 ***

INSTRUCTIONS:		TYPE OF REQUEST		INITIAL	MODIFY
1. Update your JKO profile		USER EDIPI (DOD ID) NUMBER FROM			
2. Fill in all fields to the best of your ability.		CAC USER FIRST NAME			
3. Ensure HIPAA/Cyber Awareness training dates are included.		USER MIDDLE INITIAL			
4. At bottom of request, place the name of a current user to mirror.		USER LAST NAME			
5. CAC sign and have your supervisor CAC sign. (Open file in Adobe to CAC sign).		USER ORGANIZATION			
6. In your email, please provide a phone number and a time frame to contact you to schedule your Instructor Led Training (ILT).		USER OFFICE SYMBOL/DEPARTMENT			
		USER JOB TITLE			
		USER RANK/GRADE			
		USER DEE E-MAIL ADDRESS (@MAIL.MIL)			
		USER OFFICE PHONE #			
		USER SITE LOCATION			
		USER'S PRIMARY CLINIC			
		DATE HIPAA TRAINING COMPLETED			
		DATE CYBER AWARENESS TRAINING COMPLETED			
ARE YOU A CREDENTIALLED HEALTH CARE PROVIDER? (See page 3 for resource scheduling.)		NATIONAL PROVIDER IDENTIFIER NUMBER (NPI ID)		YES	NO
		CLINIC(S)			
WILL YOU BE PRESCRIBING ORDERS?		DEA NUMBER		YES	NO
		BUSINESS FAX NUMBER (REQUIRED FOR SPI REQUEST)			
ARE YOU A CONTRACTOR?		COMPANY NAME		YES	NO
		DATE			
ARE YOU A FOREIGN NATIONAL?		CAC EXPIRATION DATE		YES	NO
ARE YOU DENTAL PERSONNEL?		Will you need to take workload and/or will appointments be scheduled with you? (i.e. dentist, dental resident, opa)		YES	NO
If you are a dentist, dental resident, hygienist, prophyl tech, efda or opa, please provide NPI number:					
Name all clinics within your scope of practice where the user will need to log in and work:					
If multiple clinics, which one is the user's primary clinic?					
If you are not a dental clinic staff member, do you have a dental clinic commander approval to provision this user?				YES	NO
INCLUDE ANCILLARY SYSTEMS?		Bed Capacity Management	Bridge	FetaLink	iAccess
INCLUDE LEGACY SYSTEMS?		CHCS	AHLTA	HAIMS	

RESOURCE PROVISIONING *******(This page is specifically for ambulatory providers only, all others please leave blank)*******

Resource and Location Group Information

Please list the **Resource Group** and **Location Group** as it appears in MHS GENESIS Scheduling

Resource Group	
Location Group	

Appointment Type Details

ASSOCIATE THE FOLLOWING VISIT TYPES

Please list all appointment types this resource will use.

Locations must already exist in MHS GENESIS. If not, please be aware this request will be delayed until the location build has been completed.

Appointment Type	Location	Resources Available	Slot Name	Proc Dur	Total Pt Dur	Total Res Dur

Template Details

N/A - Template will be created locally

Provider/Resource:

Days of the Week:

Weeks of the Month:

Start Time	End Time	Slot Name	Slot Start	Slot End	Slot Int

ELECTRONIC HEALTH RECORD - USER REGISTRATION

PRIVACY ACT OF 1974

Authority: 10 U.S.C, Section 3013.

Purpose: To authenticate that the individual is an authorized user or health care provider in the Electronic Health Record Application.

Routine users: Information may be disclosed outside of DoD agencies as outlined in AR 340-21, para 3-2 (Blanket Routine User)

Disclosure: Mandatory. Failure to provide required information may delay your access to the Electronic Health Record application.

PRIVACY ACT OF 1974

*** APPLICANT MUST READ AND SIGN ***

The purpose of this document is to verify that I have read and understood my responsibilities for safeguarding my access and the integrity of the Electronic Health Record (EHR).

The Privacy Act of 1974 imposes responsibilities to prevent misuse or compromise data concerning individuals. It has three main provisions:

- 1.CONFIDENTIALITY OF INFORMATION.** Most of the information within the EHR is sensitive, personal medical information. Only authorized people or agents are allowed to disclose this information.
- 2.DATA INTEGRITY.** Patient treatment decisions are made from the EHR information. Users of the system are responsible for ensuring that all data entered into the EHR is accurate.
- 3.DATA SECURITY.** The Privacy Act requires safeguards for confidential and secure records. This entails protective measures for preventing accidental or malicious alteration, destruction, or disclosure of PII/PHI that could affect medical care or the patient's privacy.

I am responsible for all of the following security related guidelines as laid down in DOD and DA directives. My access is unique to me. It **MUST BE KEPT CONFIDENTIAL**. Any action I make on the system may be audited by the EHR Database Administrator (DBA). I must memorize my PIN and will not make a written record of my PIN. If I suspect that someone else is using my password, I must change my password immediately and notify the EHR DBA.

I understand that I am specifically prohibited from using any other person's password. I understand that I am also prohibited from attempting to enter the system by guessing or randomly entering passwords.

I understand that my access to the EHR program does NOT, in and of itself, give me authority to disclose patient data to anyone.

I have read and understood the security guidelines given above and the necessity for safeguarding my password and the integrity of the EHR. I understand that if I divulge my password or information that is protected by the Privacy Act, I may be prosecuted under the Uniform Code of Military Justice or the United States Code (5 U. S. C., 552a (1)).

IMPORTANT --- NON-PROVIDER USERS --- IMPORTANT

As a user of the EHR application in a non-health care provider status, I am aware that the access level that I will be given may display a menu option for ordering medications. I have been advised of the command policy, which prohibits me from accessing this menu option. I also understand that I am not authorized under any circumstances to place medication orders in the EHR application.

I further acknowledge that violation of this policy will result in disciplinary action as set forth by the Commanding Officer, including immediate loss of access to the EHR application, possible dismissal and/or punishment under the Uniform Code of Military Justice

Applicant CAC Signature

Supervisor CAC Signature

Supervisor's DEE email address

Supervisor's Office Phone

Match User's Account To