TAMC FORM 30 COMPLETION INSTRUCTIONS
for REMOTE ACCESS TO CHCS/AHLTA

Applicant's request for remote access must be approved by the Information Assurance Security Officer. Upon approval by IASO, the appropriate local Trusted Agent must transcribe hard-copy information into the web-based Form e30. Allow 10 working days to complete account build from the date the TAMC Form 30 is submitted by Trusted Agent.

- System requested (CHCS, AHLTA, BOTH)
    - Check System
    - Check User Status (new, modify, etc)
- User Information
    - Legal Name
    - SSN
    - DOB
    - Gender
    - Duty phone #
    - YES/NO to previous AHLTA account
        - If yes, previous location and previous AHLTA User ID
    - Status (Active Duty, Reserves, Civilian, etc)
    - Role (Staff Provider, RN, LPN, MEDIC/Nurse Asst, etc)
    - Specialty position (Section chief, OIC, Supervisor, HN/CNS, CRNA/NP, etc)
    - Assigned Department & Duty Area at TAMC
- Provider Information
    - Provider specialty code from reference list
        - All AHLTA users require entry in this field
    - Credentials to be verified by Quality Assurance
- Department
    - Svc branch and grade
    - Supervisor name & phone #
    - MOS (active duty only)

TAMC FORM 30 COMPLETION INSTRUCTIONS
for REMOTE ACCESS TO CHCS/AHLTA

- CHCS Menus - Access is based on Role & Provider information requested above
  - Check box if account is read only
  - Special Requests/Notes for additional secondary menus and/or security keys
- AHLTA Group - Access is based on Role & Provider information
  - Check box if account is read only
  - Primary Clinic for initial acct setup
  - Special Requests/Notes for additional keys
- Training Requirements
  - Users must have proof of prior training in order to "test out"
  - Specific training requirements vary depending on role of user
- Supervisor Concurrence
  - Supervisor name, duty phone & signature required