

5 Processing the 1st E-Application for Clinical Privileges

CCQAS 2.8 provides a full online privilege request, review, and approval capability designed to support the privileging process at the facility- or unit-level. In order to realize the benefits of this capability, all individuals involved in the privileging process must have a user account in CCQAS with permissions that support their individual role(s) in the process. The following sections will describe the online privilege application process in the context of these user roles.

5.1 User Roles in the Privilege Approval Process

The following comprises the roles that are needed to process an application for clinical privileges in CCQAS 2.8:

- **Provider:** Individual provider seeking the approval of requested clinical privileges at his or her unit or facility
- **CC/MSSP/CM (Credentials Coordinator[Army]/Medical Staff Services Professional [Navy]/Credentials Manager[AF]):** Professional Affairs office staff who are responsible for ensuring providers' credentials are in order, for tracking and managing the review and approval of an application for clinical privileges, and for managing CCQAS user accounts for their facility or unit
- **CVO (Credentials Verification Office):** Credentials Verification Office staff members or other credentialing personnel who perform the primary source verification (PSV) of provider credentialing data; PSV function may also be performed by individuals who are assigned the CC/MSSP/CM role
- **Reviewer:** Clinical staff privileging committee members who have been assigned the responsibility for reviewing and recommending actions on applications for privileges. Reviewers may include the provider's supervisor, the specialty, service or section chief, the department chair, and/or the members and chair of the executive committee of the medical (dental) staff (ECOMS/ECODS)
- **PA (Privileging Authority):** Usually the medical treatment facility (MTF) commander or other designated person who is responsible for final approval of applications for clinical privileges
- **CLP Administrator:** The individual who has been assigned responsibility for managing the privilege catalog at his or her unit or facility. He or she will also be responsible for indicating on the catalog whether his/her facility or unit can or cannot support each privilege item. Depending on the size of the MTF or other determining factors, this role may also be played by the CC/MSSP/CM. The privilege catalog was based on *common language privileging*, hence the abbreviation, "CLP"

Additional roles will be assigned to individuals who are responsible for generating and reviewing performance assessments for Providers and reviewing and approving physician state license waiver requests:

- **PAR Evaluator:** Supervisors, service chiefs, department chairs or other clinical personnel who are responsible for completing and submitting a performance assessment report (PAR) on a provider
- **PAR Reviewer:** Clinical staff members who are responsible for reviewing a PAR submitted by a PAR evaluator
- **SLW Endorser:** Person at the MTF (usually the privileging authority) or Command (usually the Command Surgeon) who is responsible for review and approval of physician state license waiver (SLW) requests. Authority to approve the SLW is usually delegated to such an individual from the Office of the Assistant Secretary of Defense for Health Affairs (OASD/HA)

In CCQAS 2.8, one individual may have multiple roles in the privileging process. For example:

- A Provider may also be a Reviewer (though CCQAS will not allow a Provider to act as Reviewer for his or her own privilege application)
- A CC/MSSP/CM may also be a CLP Administrator
- A Reviewer may also be a PAR Evaluator
- The Privileging Authority may also be the SLW approver (endorser)

It is also important to note that some roles will not be involved in the processing of every privilege application. For example:

- If the CC/MSSP/CM at a facility performs the primary source verification of all the provider's credentials, then the CVO role will not be involved in the application review process.
- The State License Waiver Endorser will not be involved in the application review process if no state license waiver is generated by the system.
- A PAR is not required if an application for modification of privileges is being processed.

Each role in CCQAS is differentiated from the others according to the permissions assigned to the user's account. If an individual is responsible for multiple roles, his/her user account will be assigned the permissions associated with all roles for which he/she is responsible.

5.2 The Work List

CCQAS 2.8 provides a work list to organize each user's work list items, or tasks. The work list (Exhibit 5.2-1) is the first screen each user will see upon logging into CCQAS.

WorkList for W0Q3AA, BEAUMONT ARMY MED CTR

Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date
Setup PAR	CC/CM/MSSP	N/A	NIP, Coffee (Civilian)	Transfer (ICTB)		08/12/2006	
Setup PAR	CC/CM/MSSP	N/A	MUSKATEERS, THREE (Military)	Transfer (ICTB)	Medical Corps	08/12/2006	
Privileging Acknowledgment Received	CC/CM/MSSP	GUMBO, SHRIMP (Provider)	GUMBO, SHRIMP (Military)	1st E-App	Medical Service Corps	08/11/2006	
Setup PAR	CC/CM/MSSP	N/A	RIPPLE, FUDGE (Military)	1st E-App	Medical Corps	08/10/2006	
Setup PAR	CC/CM/MSSP	N/A	RIPPLE, FUDGE (Military)	1st E-App	Medical Corps	08/10/2006	
Setup PAR	CC/CM/MSSP	N/A	RIPPLE, FUDGE (Military)	1st E-App	Medical Corps	08/10/2006	
Privileging Acknowledgment Received	CC/CM/MSSP	Jaeger, Mint (Provider)	Jaeger, Mint (Military)	Transfer (ICTB)	Medical Corps	08/10/2006	

Exhibit 5.2-1. The Work List Screen for the CC/MSSP/CM

The following are important features of the work list screen:

- The work list will default to display tasks with “**Status** = *Open*”, which means the user needs to take some type of action with respect to the listed application
- The work list will display old tasks that have already been completed, by selecting “*Closed*” from the **Status** pick list
- For those users that have multiple roles in the privileging process, they may display all tasks in the same list by selecting “**Role** = *All*”; conversely, they may display only those tasks associated with a particular role by selecting the desired role from the pick list
- The work list will default to display tasks for the past 30 days; the date range for displaying work list items may be changed by entering the desired **Start** and **End** dates and clicking the <Filter> button.

CCQAS will send an email notification to a user each time a new task is added to his or her work list. Further discussion of the notifications function is discussed in the following section.

5.3 Notifications

Efficient and timely processing of the online application package requires coordination between all individuals involved with the privileging process without relying on or the need for face-to-face communication. To facilitate the online privileging process, automated notifications were built into CCQAS 2.8. The notifications consist of automated email messages that are sent to individuals when action on a privilege application or other CCQAS-managed object is required. This notification will be sent to the email address entered into CCQAS when the user account was initially created. It is important that any changes to this email address be updated by either the user or the MTF Administrator to ensure these notifications continue to reach the targeted individual. Directions for updating user account information are provided in Section 3.1.

An email notification is automatically generated by CCQAS when the user receives a new task. While this functionality should prove helpful for Providers, Reviewers, and other roles that may not use CCQAS on a daily basis, daily users of CCQAS, such as a CC/MSSP/CM may not need these notifications and wish to disable them. A CC/MSSP/CM may disable or turn off his or her own email notification function by

clicking on the “System” main menu, then “Messaging” (Exhibit 5.3-1), and then “Email Notification” (Exhibit 5.3-2).

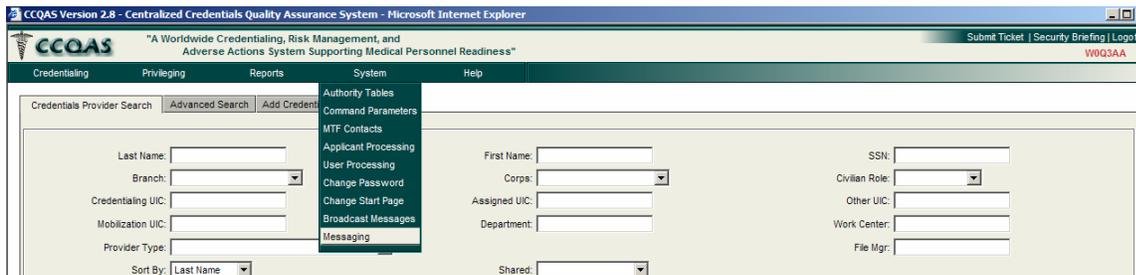


Exhibit 5.3-1. The Messaging Menu Item

The email notifications may be turned off by following the instructions on the screen.



Exhibit 5.3-2. Disabling the Email Notification for the CC/MSSP/CM

Note: The notification function may only be disabled for the CC/MSSP/CM role. CCQAS does not allow notifications to be disabled for Providers, Reviewers, or other roles in the privileging process.

5.4 Types of Privilege Applications

CCQAS classifies privilege applications according to the provider’s privileging status at a given facility or unit.

Application Type	Description
1 st E-Appl Modification	The first online application that is submitted by a provider in CCQAS
Transfer (ICTB)	An application for a modification of clinical privileges that were previously granted or approved through the CCQAS workflow process at the assigned duty station
Transfer (PCS)	An application for privileges at a temporary duty location (gaining facility) after privileges were previously granted through the CCQAS workflow process at the assigned location (parent facility). Simply referred to as “ICTB” because this transfer requires an inter-facility credentials brief (ICTB)
Renewal	Following a permanent change of station (PCS), an application for privileges at the new duty location (gaining facility) after privileges were granted through the CCQAS workflow process at the previously assigned duty station (losing facility).
	An application for renewal of clinical privileges which are due to expire, and which were previously granted through the CCQAS workflow process at the same duty station

Exhibit 5.4-1. Types of Privilege Applications

All providers, regardless of their current privileging status or eligibility for privileging, will have to submit a CCQAS 2.8 electronic privilege application for the first time. This first electronic application may be any one of the other application types indicated in Exhibit 5.4-1, but it will be designated as “1st E-App!” on the Work List. After an application is submitted and processed through the CCQAS workflow for the first time, all subsequent applications will be identified as one of the other application types.

New clinical support staff (CSS) personnel and others who typically are not eligible for privileging may also complete and submit their 1st E-Application to ensure their credentials information is completely and correctly entered into the CCQAS database. Modification and Renewal applications generally only apply to privileged providers, but CCS who are military personnel may also have Transfer (ICTB or PCS) applications.

A record of all privilege applications processed through CCQAS is maintained on the Applications screen and may be accessed by clicking on “My Applications” tab (Exhibit 5.4-2).

Provider	Application Type	Application Status	Provider Phone	App Submitted	Priv Effective	Priv Expiration
CHEESE, HAM	Transfer (ICTB)	Complete	(310) 339-8845	08/08/2006	08/08/2006	08/08/2006
GUMBO, SHRIMP	1st E-App	Complete	(210) 207-2722	08/11/2006	08/11/2006	08/10/2007
Jeager, Mint	Transfer (ICTB)	Complete	(210) 339-8845	08/08/2006	08/08/2006	11/08/2006
MONKEY, CHUNKY	1st E-App	Complete	(702) 339-8845	08/10/2006	08/10/2006	
RIPPLE, FUDGE	1st E-App	Complete	(210) 221-7911	08/09/2006	08/10/2006	08/10/2006

Exhibit 5.4-2. My Application Tab

The following are important features of the My Application screen:

- The user may search for a particular provider application by entering the **Provider Last Name** and clicking the <Filter> button
- The Application screen will default to display applications submitted in the past year; the date range for displaying submitted applications may be changed by entering the desired **Start** and **End** dates and clicking <Filter>
- The application may be opened and viewed by selecting “Open” from the hidden menu of actions, or by double-clicking on the line item
- Applications that have previously been approved, terminated, or are otherwise not active will be presented in read-only format

A list of all applications in “pending” or “terminated” status are listed on the “Pending Applications” tab Exhibit 5.4-3).

Provider	Application Type	Status	Provider Phone	Application Task Initiated	Provider Started Completing	Number of Days Completing
BANANA, YELLOW	1st E-App	Terminated	210913249	08/10/2006	08/10/2006	11
CHERRY, CHOCOLATE	1st E-App	Pending	(310) 333-4444	08/15/2006	08/15/2006	6
Jeager, Mint	Modification	Pending	(210) 339-8845	08/10/2006	08/10/2006	11
MUSKATEERS, THREE	Transfer (ICTB)	Terminated	574-8290	08/09/2006	08/09/2006	12
MUSKATEERS, THREE	Transfer (ICTB)	Pending	574-8290	08/09/2006	08/09/2006	12
NIP, Coffee	Transfer (ICTB)	Pending	(210) 339-8845	08/09/2006	08/09/2006	12
RIPPLE, FUDGE	Renewal	Terminated	(210) 221-7911	08/10/2006	08/10/2006	11
RIPPLE, FUDGE	Renewal	Terminated	(210) 221-7911	08/10/2006	08/10/2006	11
RIPPLE, FUDGE	Renewal	Terminated	(210) 221-7911	08/10/2006	08/10/2006	11
RIPPLE, FUDGE	Renewal	Pending	(210) 221-7911	08/10/2006	08/10/2006	11
Ripple, Fudge	1st E-App	Terminated	(210) 221-7911	08/08/2006	08/08/2006	13
Ripple, Fudge	1st E-App	Terminated	(210) 221-7911	08/08/2006	08/08/2006	
Vanilla, Bean	1st E-App	Pending	(202) 207-5833	08/17/2006	08/17/2006	4
banana, yellow	1st E-App	Pending	(210) 916-4444	08/10/2006	08/10/2006	11

Exhibit 5.4-3. Pending Applications Tab

Applications are considered “Pending” if they were generated during the date range specified at the top of the tab, but have not yet been completed and submitted by the provider. Applications in “Terminated” status are applications that were closed by the CC/MSSP/CM during the specified date range, prior to completion of the review and approval process.

5.5 Initial Review of a Privilege Application

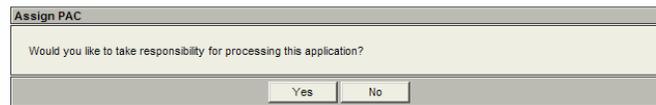
Once a provider has E-signed and submitted their application online, the CC/MSSP/CM will receive a new work list item with “Task = *Application Ready for Review*” . The provider’s application may be viewed from the work list by selecting “Open” from the hidden menu (Exhibit 5.5-1), or double-clicking anywhere on the record line item.

Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date
Application Ready for Review Open	CC/MMSSP	PERCE, BENJAMIN (Provider)	PERCE, BENJAMIN (Military)	1st E-App	Medical Corps	08/07/2006	08/07/2006

Exhibit 5.5-1. Work List Task – Application Ready for Review

CCQAS will return a message window (Exhibit 5.5-2), asking the CC/MSSP/CM if he/she will take responsibility for processing the application. This feature was built into CCQAS to accommodate larger facilities and units in which multiple staff members share the credentialing and privileging workload. If the CC/MSSP/CM is the only staff member at his/her facility or unit who manages privilege applications, he/she will select <Yes>. If the privileging workload is shared across staff members, the CC/MSSP/CM will only respond with <Yes> for those applications for which he/she will be personally responsible. For larger facilities with multiple professional affairs office staff members,

division of workload is an internal office business process or decision and is outside of the purview of CCQAS.



Assign PAC

Would you like to take responsibility for processing this application?

Yes No

Exhibit 5.5-2. The Assign PAC Screen

In order to move forward in the review process with this application, the CC/MSSP/CM must click <Yes>. If <No> is selected, the work list item will remain active in all CC/MSSP/CM's work list for the facility or unit until ownership of the application is accepted by one of them, at which time, the item will disappear from the work list of the other CMs/MSSPs/CCs, and is viewable only in the work list of the one accepting responsibility for it.

Accepting responsibility for processing the application has several implications:

- The accepting CC/MSSP/CM becomes the sole custodian of the privileging application and will be the only credentialing staff member at his or her facility or unit who may route the application for PSV, review, or approval; return the application to the provider; or terminate the processing of the application
- The accepting CC/MSSP/CM will be the only credentialing staff member that receives email notifications or work list items pertaining to the privilege application
- The accepting CC/MSSP/CM may reassign the application to another CC/MSSP/CM in his/her unit or facility at any time during application processing, but, in doing so, will lose custody of the application once it is reassigned

Once the CC/MSSP/CM accepts responsibility for the application by clicking on <Yes>, the E-Application will be returned as a series of tabs.

5.5.1 The Provider Summary Tab

The Provider Summary (Exhibit 5.5-1) is the first tab in the privilege application. This tab displays demographic information that the provider entered into the "Profile", "Identification" and "Contact" sections of the electronic application.

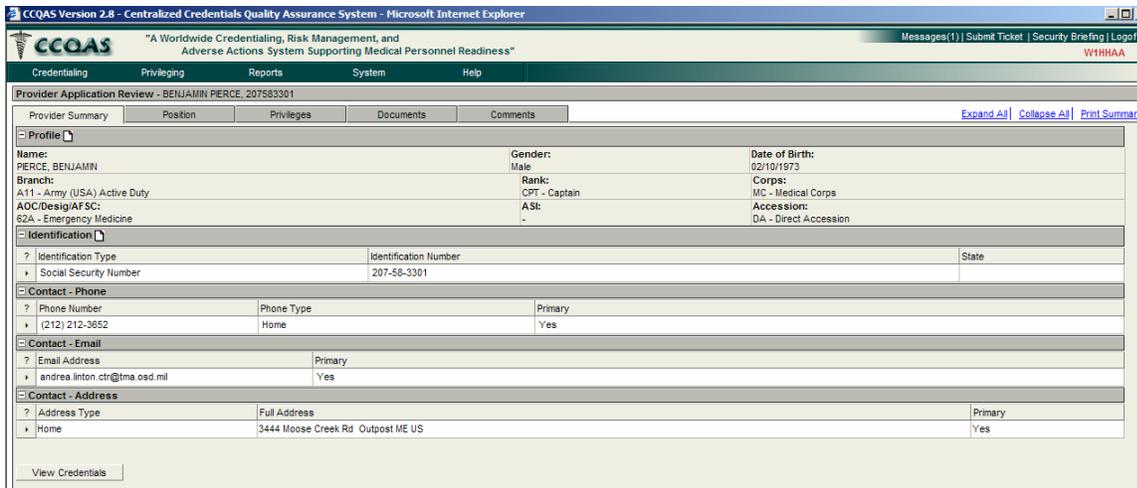


Exhibit 5.5-3. The Provider Summary Tab

The remainder of the credentials information in the provider's application may be viewed by clicking the <View Credentials> button.

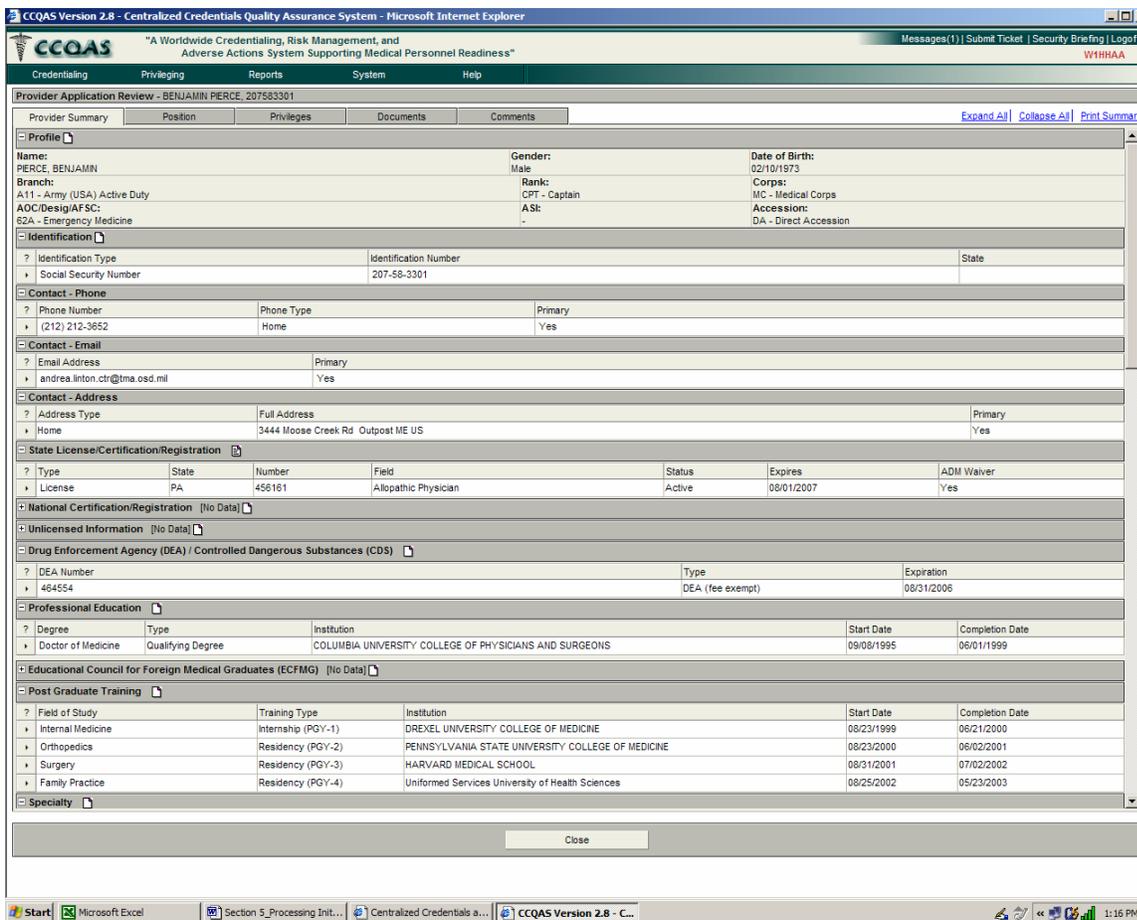


Exhibit 5.5-4. The Expanded Provider Summary Tab

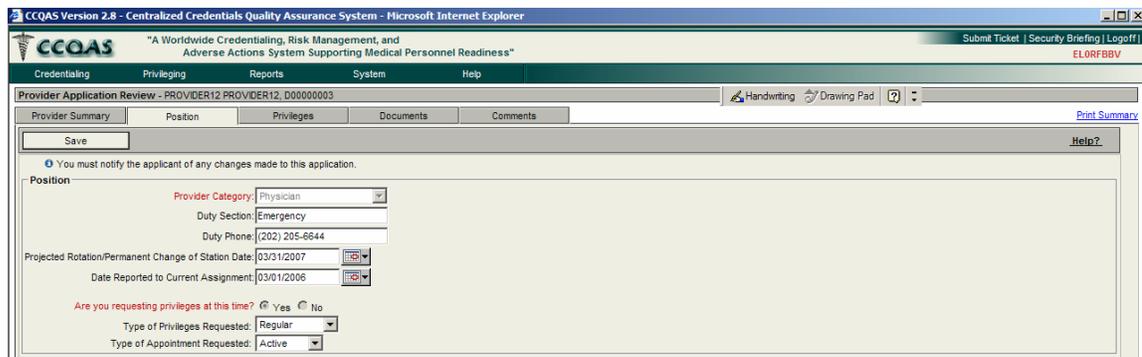
The screen will refresh to display the full credentials record for the provider. The following are important features of the expanded Provider Summary screen:

- The credentials information is presented in read only format; if changes or additions are required, the CC/MSSP/CM must return the application to the provider who makes the appropriate changes as instructed by the CC/MSSP/CM through either a comment within the application itself, or outside of the system through a telephone call or email
- Specific sections in the application include data fields for documenting PSV information; these fields may not be populated until the application is submitted for PSV
- Each section of the application may be expanded or collapsed by clicking the [+] or [-] to the left of the section label
- A hardcopy listing of the whole electronic application package may be printed by clicking <Print Summary> in the upper right corner of the Provider Summary tab
- The CC/MSSP/CM may add a note to the reviewers by clicking on the empty note (□) icon for a section. Once a note is added, the empty note icon (□) will become a filled note (■) icon. Only the CC/MSSP/CM has this capability. When routed to the reviewers, the filled note icon is replaced by a red flag icon (■) to indicate to the reviewers that the CC/MSSP/CM has added a note and that the reviewer needs to pay particular attention to the section. Notes entered by the CC/MSSP/CM will be viewable by the Reviewers during the review process, but will not be visible to the provider

Prior to processing the application, the CC/MSSP/CM should review all credentials information entered by the provider for accuracy and completeness.

5.5.2 The Position Tab

The Position tab (Exhibits 5.5-5 and 5.5-6) is the second tab in the privilege application. This tab displays the information that the provider entered in the “Position” section of the electronic application.



The screenshot displays the CCQAS web application interface. At the top, the browser title is "CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer". The application header includes the CCQAS logo and the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". Navigation tabs include "Credentialing", "Privileging", "Reports", "System", and "Help". The main content area is titled "Provider Application Review - PROVIDER12_PROVIDER12_D00000003" and features a "Save" button and a "Help?" link. A message states: "You must notify the applicant of any changes made to this application." The "Position" section contains the following fields:

- Provider Category: Physician
- Duty Section: Emergency
- Duty Phone: (202) 205-6644
- Projected Rotation/Permanent Change of Station Date: 03/31/2007
- Date Reported to Current Assignment: 03/01/2006
- Are you requesting privileges at this time? Yes (selected) / No
- Type of Privileges Requested: Regular
- Type of Appointment Requested: Active

Exhibit 5.5-5. The Position Tab for Navy and Air Force

Exhibit 5.5-6. The Position Tab for Army

The Position tab enables the CC/MSSP/CM to quickly determine the type of provider who submitted the application and whether or not clinical privileges are being requested with the application. If the provider is a member of the clinical support staff (CSS), his/her application will not include a request for clinical privileges.

The remainder of the fields on the Position tab are editable by the CC/MSSP/CM. If the CC/MSSP/CM changes any information previously entered by the provider, the provider should be notified regarding the nature and justification for the change; otherwise, the CC/MSSP/CM may return the application to the provider for him to make the change as instructed.

5.5.3 The Privileges Tab

The Privileges tab (Exhibit 5.5-7) lists all the privileges associated with the specialty or specialties in which the provider is requesting privileges, and the provider's requested delineation for each privilege item. For Army and Air Force facilities, delineations are either "Fully Competent", "With Supervision", or "Not Requested." For Navy facilities, delineations are either "Yes" or "No."

Note: The CC/MSSP/CM or CLP Administrator should already have configured the privilege catalog to indicate which privileges his/her facility can or cannot support and the system will automatically display non-supported privileges as "Not Supported" when the application is routed to the reviewers. Providers, however, should be instructed to request all privileges they are qualified to perform, regardless of what is or is not supported.

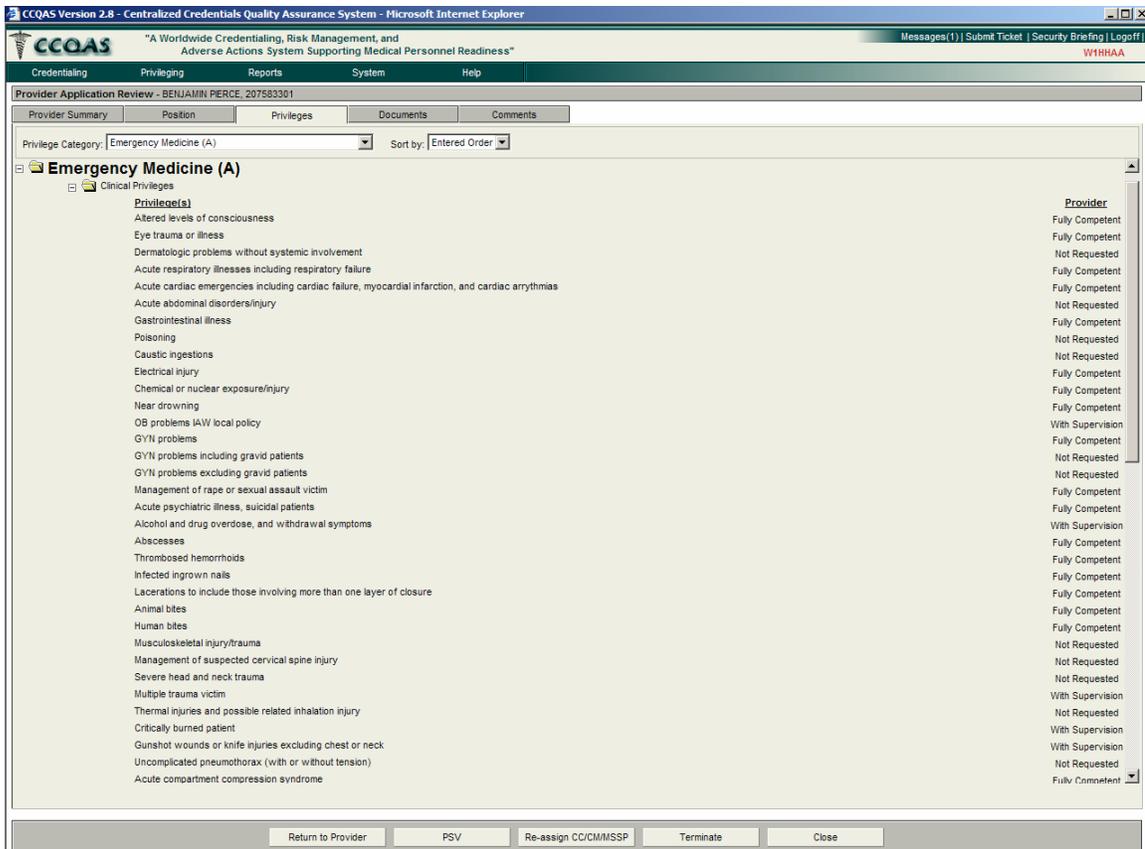


Exhibit 5.5-7. The Privileges Tab for Army Emergency Medicine

The following are important features of the Privileges tab:

- All privilege delineations will be read-only to the CC/MSSP/CM; if changes in privilege delineations are needed, the CC/MSSP/CM must return the application to the provider with a request to make the appropriate changes
- Privilege lists contained within folders (📁) may be expanded or collapsed by clicking the [+] or [-] to the left of the icon
- A paper copy of the whole application package may be obtained by clicking the **Print Summary** link in the upper right corner of the Provider Summary tab
- The Privileges tab will be inactive for applications submitted by CSS personnel or providers who are not requesting clinical privileges with their application

The CC/MSSP/CM should review the “Privilege Category” drop-down list (see Exhibit 5.5-7) on the Privileges tab to identify all specialties for which the provider is requesting clinical privileges. This information will be needed when assigning individuals to review the application.

5.5.4 The Documents Tab

CCQAS 2.8 enables users to upload documents that are needed to support the privileging process and maintain current credentials records.

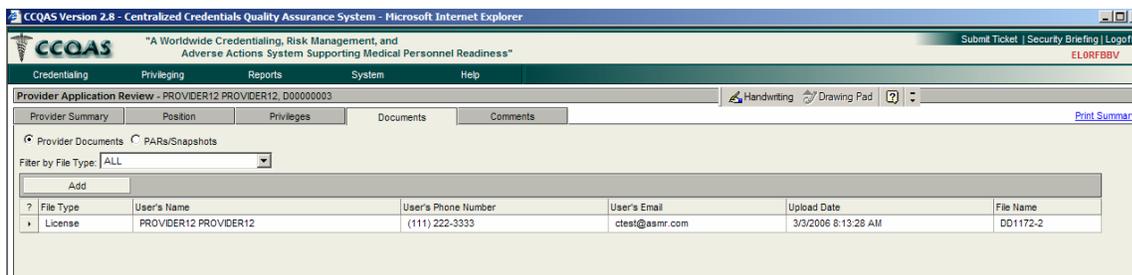


Exhibit 5.5-8. The Documents Tab

The following are important features of the Documents tab:

- In order to be uploaded into CCQAS, each individual document must be 1MB (megabyte) or less in size and have a *pdf*, *jpeg*, or *gif* file extension
- **Provider Documents** or **PARs/Snapshots** documents may be displayed by selecting the appropriate radio button at the top of the tab (Exhibit 5.5-8)
- The list of documents associated with the application may be searched by selecting the desired document type from the **Filter by File Type** pick list
- The summary line for each uploaded document includes the type of document, when it was uploaded and by whom, and the name of the file that was uploaded
- The document may be viewed by double-clicking on the line item, after which a “File Download” dialog box will pop up. Click on **<Open>** to view the document, or click on **<Save>** to save the document in your hard drive or some other storage device
- The **User Name** reflects the individual who uploaded the document to the application and the **Upload Date** reflects the date and time the document was originally uploaded

CCQAS allows providers to upload specific types of documents into their application prior to submitting it, including:

- License, certification and/or registration
- Diploma
- Specialty Board Certifications
- ECFMG Certification
- Training Certificates
- CMEs/CEUs (continuing education training documents)
- Proofs of contingency training (BLS, ACLS, PALS, C4, CBRNE, etc.)

Any document uploaded into the application by the provider will be listed on the Documents tab when the CC/MSSP/CM receives the application. The CC/MSSP/CM may also upload a provider’s documents into CCQAS, as well as other document types that the provider does not have permission to upload, by clicking the **<Add>** button (see Exhibit 5.5-8).

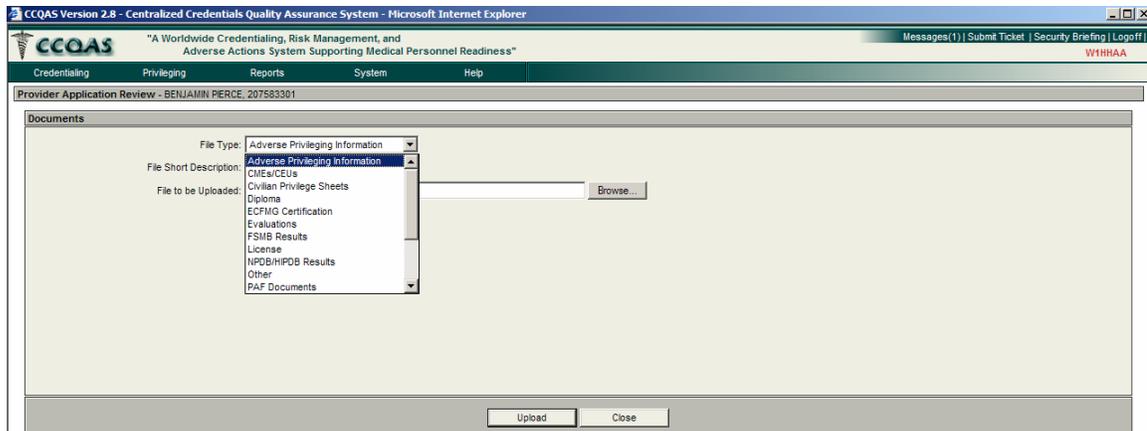


Exhibit 5.5-9. The Add Documents Screen

The provider will have visibility of all documents uploaded in CCQAS regardless of who uploaded the document into his/her application. Prior to the submission of an application, the provider may delete documents he uploaded and associated with his application. Once an application is submitted, PSV'd and routed for review, the attached documents may no longer be deleted from an application. Once the application is routed for review, documents uploaded by the CC/MSSP/CM can no longer be deleted.

5.5.5 The Comments Tab

The Comments tab will display a summary record for all comments entered into the application as it proceeds through the review process.

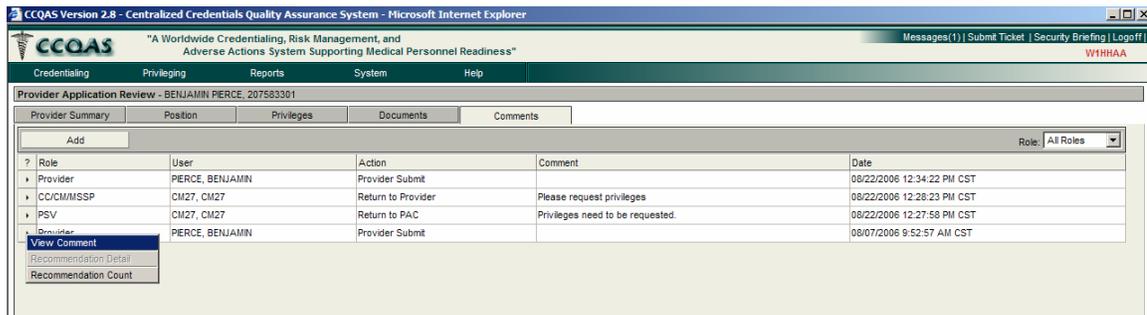


Exhibit 5.5-10. The Comments Tab

The complete record of the comments may be viewed by selecting “View” from the hidden menu of actions for the summary record. A new comment may be added by clicking the <Add> button (Exhibit 5.5-11).

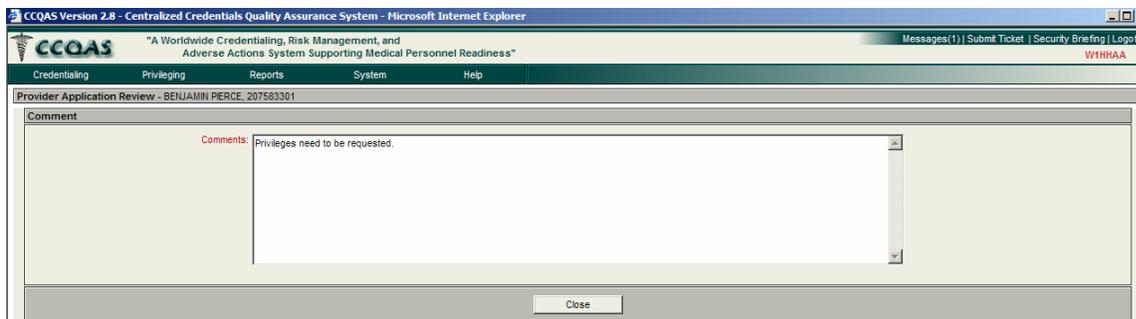


Exhibit 5.5-11. The Add Comments Screen

Comments entered into the submitted application may or may not be viewable by the provider, depending upon when they were entered. Comments that will be viewable by the provider include:

- Comments entered by the provider when he/she submits his/her application
- Comments entered by the CC/MSSP/CM if/when an application is returned to a provider with a request for edits or additional information on the application

The provider will not have visibility of comments generated during the application review process, such as those entered by the CC/MSSP/CM on the “Provider Summary” screen or comments entered by reviewers when they issue their recommendation for or against approval of the application. All review comments will be maintained as part of the historical record for the application, but viewable only to those directly involved in the review process.

5.5.6 Taking Action on a Privilege Application

After reviewing the privilege application for completeness, the CC/MSSP/CM is ready to take action on the application. To do so, they will select one of the buttons provided at the bottom of any tab within the application package (Exhibit 5.5-12):

- **<Return to Provider>** will route the application back to the provider who originally submitted it; the CC/MSSP/CM is required to enter comments or instructions to the provider when selecting this option. The provider will then receive an email notification and a task, instructing him/her to access CCQAS, review the CC/MSSP/CM comments and modify the application accordingly
- **<PSV>** will submit the application for primary source verification which may be done by the CC/MSSP/CM or by a CVO function. Further processing of the application may not be performed until the PSV process has been completed
- **<Re-assign CC/MSSP/CM>** will enable the user to turn over custody of the record to another CC/MSSP/CM in his/her respective facility or unit (see Section 5.5.7)
- **<Terminate>** will halt the application process immediately. The application may no longer be processed, but a read-only copy of the terminated application will be retained by CCQAS and may be accessed from the Applications tab

- <Close> will close the application which may then be reopened later. Clicking this button will return the user to his/her work list

5.5.7 Reassigning Ownership of an Application to Another CC/MSSP/CM

If a CC/MSSP/CM has already accepted responsibility for an application and determines that the application should be handled by another CC/MSSP/CM in the same facility or unit, the custody of the application may be transferred to the other individual by clicking the <Reassign CC/MSSP/CM> button (Exhibit 5.5-12).

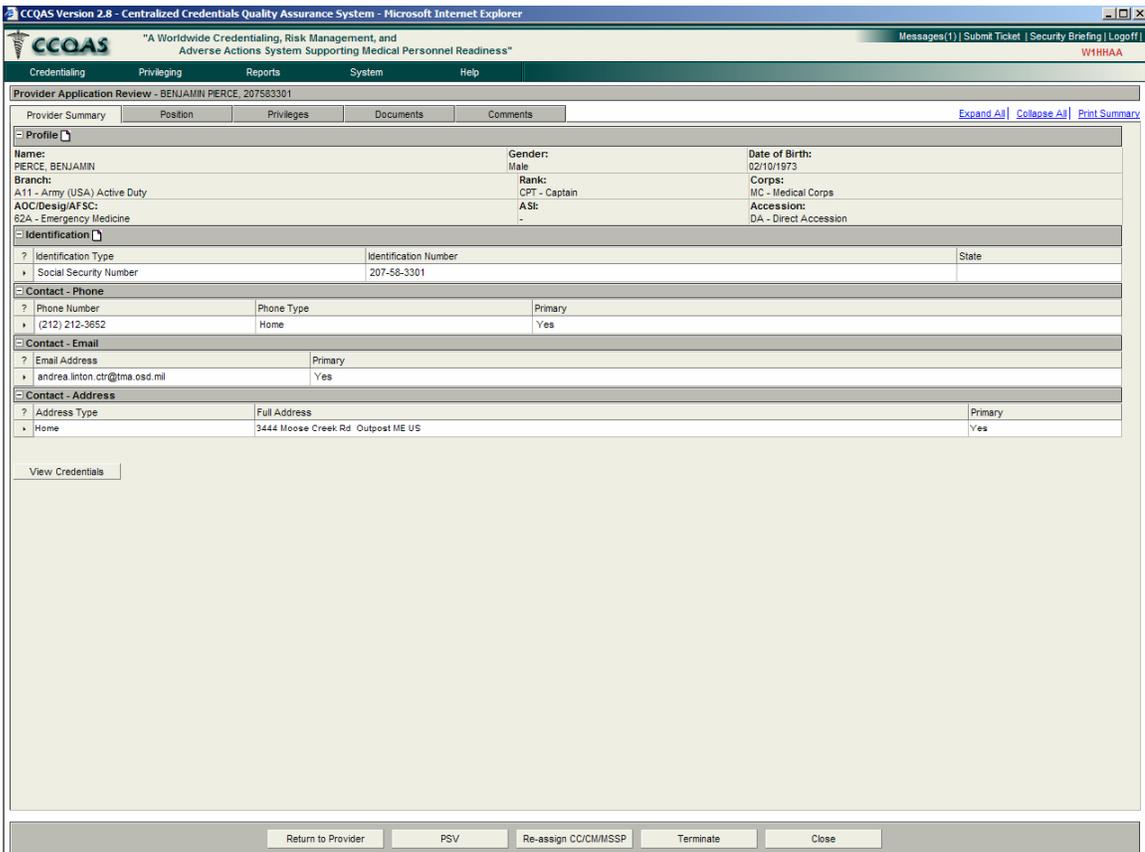


Exhibit 5.5-12. The Reassign CC/MSSP/CM Button

A window will be returned Exhibit 5.5-13), which contains a pick list of all available CMs/MSSPs/CCs in the facility or unit to whom responsibility for the record may be transferred.

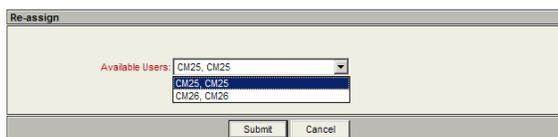


Exhibit 5.5-13. The Reassign Screen

Once <Submit> is clicked, full custody of the application will be transferred to the individual selected.

5.5.8 Taking Ownership of an Application from Another CC/MSSP/CM

The **Application Reassignment** function may be used in situations where ownership of one or more privilege applications must be transferred to a different CC/MSSP/CM, but the CC/MSSP/CM who is currently responsible for the application(s) is not available to initiate the reassignment. The <Application Reassignment> button is located at the bottom of the work list tab (Exhibit 5.5-14).

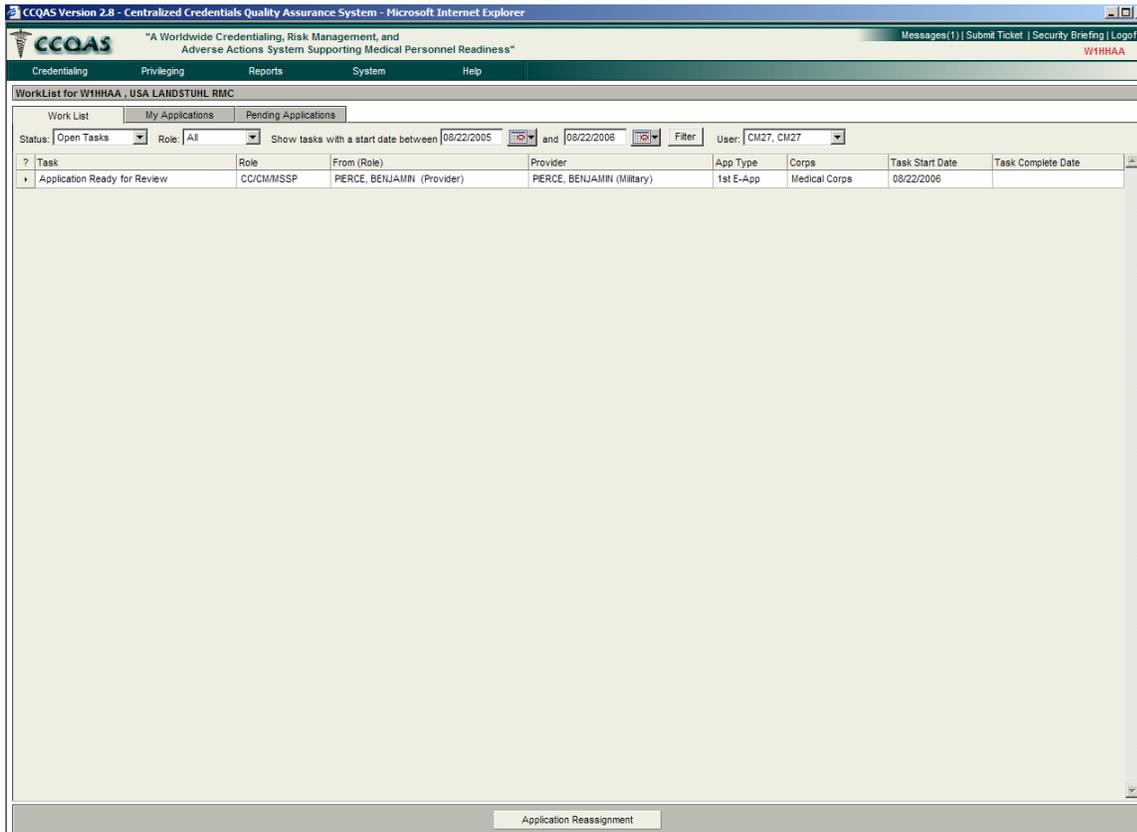


Exhibit 5.5-14. Application Reassignment Button

Upon clicking <Application Reassignment>, the Application Reassignment screen is returned (Exhibit 5.5-15), showing all applications submitted within the last year that are associated with the user's facility or unit.

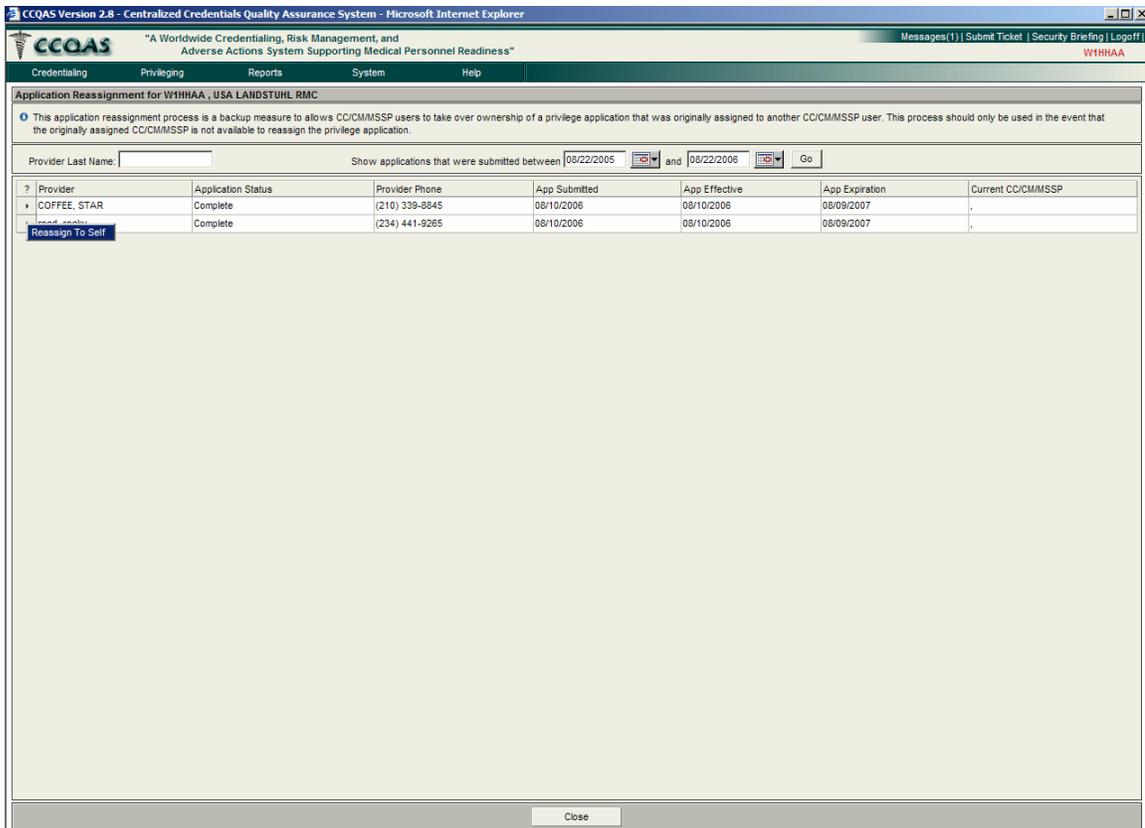


Exhibit 5.5-15. The Application Reassignment Screen

The following are important features of the Application Reassignment screen:

- The user may search for a particular provider’s application by entering the **Provider Last Name** and clicking the <Go> button at the top of the page
- The Application screen will default to display applications submitted in the past year; the date range for displaying submitted applications may be changed by entering the desired **Start** and **End** dates and clicking <Go>
- Custody of an application is obtained by selecting “Reassign to Self” from the hidden menu of actions (see Exhibit 5.5-15)

The Application Reassignment functionality will only allow applications to be reassigned to another CC/MSSP/CM within the facility or unit where the application was submitted. A CC/MSSP/CM may not take custody of a privilege application in a different facility or unit for which they do not have the appropriate permissions to function in the role of CC/MSSP/CM.

5.6 Routing a Privilege Application for Primary Source Verification

Once the CC/MSSP/CM has reviewed the application package and determined that it is ready for processing, he/she may submit the application for primary source verification by clicking the <PSV> button (see Exhibit 5.5-12).

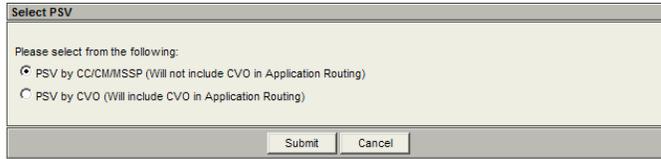


Exhibit 5.6-1. The Select PSV Screen

CCQAS will return a message window (Exhibit 5.6-1), asking whether the PSV function will be performed by the CC/MSSP/CM or a CVO role. The user will select the appropriate option and click <**Submit**>.

- If “**PSV by CC/MSSP/CM**” is selected, a new work list item will be generated for all CC/MSSP/CM personnel in the facility or unit who hold PSV permissions; one of those individuals must then assume responsibility for the application prior to conducting the PSV
- If “**PSV by CVO**” is selected, a new work list item will be generated for all individuals who have PSV permissions in the designated CVO unit; one of those individuals in the CVO unit must assume responsibility for the application prior to conducting the PSV
- Regardless of who performs the PSV function, the individual conducting the PSV maintains ownership of the application until PSV is completed; further processing of the application may not be performed until all required PSV has been completed

The processes for primary source verification of the privilege application are addressed in the following sections.

5.7 Primary Source Verification of a Privilege Application by CC/MSSP/CM

When “**PSV by CC/MSSP/CM**” is selected as the means for primary source verification, a new task will be generated for all individuals who have permissions to perform PSV functions for their facility or unit. The application may be viewed from the work list by selecting “Open” from the hidden menu, or double-clicking anywhere on the record line. CCQAS will return a message window (Exhibit 5.7-1), asking the CC/MSSP/CM if they will take responsibility for the PSV of the application. This feature was built into CCQAS to accommodate larger facilities and units, in which multiple credentials staff members share the PSV workload.



Exhibit 5.7-1. The Assign PSV Screen

Once the CC/MSSP/CM has accepted responsibility for the PSV of the application, the application package will be returned as a series of tabs (Exhibit 5.7-2). The first tab will be the “Provider PSV Summary” tab.

CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"

Messages(1) | Submit Ticket | Security Briefing | Logout | WJHHAA

Credentialing Privileging Reports System Help

Prime Source Verification (PSV) for BENJAMIN PIERCE

Provider PSV Summary Privileges Documents Comments [Expand All](#) [Collapse All](#) [Print Summary](#)

Profile

Name:	PERCE, BENJAMIN	Gender:	Male	Date of Birth:	02/10/1973
Branch:	A11 - Army (USA) Active Duty	Rank:	CPT - Captain	Corps:	MC - Medical Corps
AOC/Desig/AFSC:	62A - Emergency Medicine	AS:	-	Accession:	DA - Direct Accession

Identification

Identification Type	Identification Number	State
Social Security Number	207-56-3301	

State License/Certification/Registration **Verified**

Update	State	Number	Field	Status	Expires	ADM Waiver	Verified
Letter	PA	456161	Alopathic Physician	Active	08/01/2007	Yes	No

National Certification/Registration [No Data] **Completed**

Unlicensed Information [No Data]

Drug Enforcement Agency (DEA) / Controlled Dangerous Substances (CDS)

DEA Number	Type	Expiration
464554	DEA (fee exempt)	08/31/2006

Professional Education **Verified**

Degree	Type	Institution	Start Date	Completion Date	Verified
Doctor of Medicine	Qualifying Degree	COLUMBIA UNIVERSITY COLLEGE OF PHYSICIANS AND SURGEONS	09/08/1995	06/01/1999	08/10/2002

Post Graduate Training **Verified**

Field of Study	Training Type	Institution	Start Date	Completion Date	Verified
Internal Medicine	Internship (PGY-1)	DREXEL UNIVERSITY COLLEGE OF MEDICINE	08/23/1999	06/21/2000	08/08/2002
Orthopedics	Residency (PGY-2)	PENNSYLVANIA STATE UNIVERSITY COLLEGE OF MEDICINE	08/23/2000	06/02/2001	08/21/2001
Surgery	Residency (PGY-3)	HARVARD MEDICAL SCHOOL	08/31/2001	07/02/2002	08/25/2002
Family Practice	Residency (PGY-4)	Uniformed Services University of Health Sciences	08/25/2002	05/23/2003	06/27/2003

Specialty **Verified**

Specialty	Sub Specialty	Specialty Level	Certified Date	Expiration Date	Verified
Emergency Medicine	Emergency Medical Services	Board Certified	08/09/2004	08/09/2007	01/06/2005

Malpractice Coverage

Insurance/Contractor Name	Policy Number	Policy Expires Date	Address
Geico	456165	08/19/2007	

Clinical Appointments

Name	Start Date	End Date
Massachusetts General		

Academic Appointments

Name	Start Date	End Date

Exhibit 5.7-2. The Provider PSV Summary Screen

The Provider PSV Summary screen will display expanded sections of the privilege application that require PSV action. Important features of the Provider PSV Summary screen include:

- Sections of the application which contain no data will automatically be collapsed and display “(No Data)” next to the section header
- All sections of the application may be expanded or collapsed by clicking <Expand All> or <Collapse All>, respectively, in the upper right corner of the screen
- Individual sections of data may be expanded or collapsed by clicking [+] or [-], respectively, to the left of the section header
- Sections of the application which contain data will display summary lines for each record entered
- Comments may be associated with each section of the application by clicking the empty notes icon (📝); the presence of comments for that section will be indicated by the filled notes icon (📝)
- The presence of a “Verified” checkbox on the right side of the screen indicates the sections of the application that contain data requiring PSV; once the PSV of that section is complete, CCQAS will autopopulate the “Verified” box with a check mark

- A paper copy of the whole application package may be obtained by clicking <Print Summary> in the upper right corner of the Provider Summary tab

The user may view the details and/or document the PSV information for each credential by selecting “Update” from the hidden menu, or double-clicking on the record line.

Exhibit 5.7-3. The PSV Information Section

The “PSV Information” block (see Exhibit 5.7-3) of each section requiring PSV should be completed as the individual credential is being verified according to the method of verification that is used. Any unusual circumstances surrounding the credential or the verification of the credential should be noted in the **Remarks** box. The user may edit information pertaining to the credential being verified, but they may not edit information that uniquely identifies the credential. Following PSV of the credential, the user selects <Save> and then <Close> to return to the PSV Summary screen. The name and position of the user who conducted the PSV will automatically be recorded on PSV Information block after all PSV information have been entered and saved.

Note: In the PSV Information block, different data fields are required depending on the PSV “**Method**” radio button selected. The PSV Information block should be populated as completely as possible according to the PSV method used.

Once all required PSV have been completed in the credentials sections of the application, the **Request Query** box on the NPDB section (Exhibit 5.7-4) of the application will become enabled. The CC/MSSP/CM will then check the **Request Query** box. This action will result in the inclusion of the provider’s name and information in NPDB batch queries that is generated by CCQAS to perform NPDB queries. When the system has included the provider’s name in the batch query report, it will automatically uncheck **Request Query** and check the **Query Result Pending** box and place the corresponding date in the **Last Query Date** field. When the query results are received, the CC/MSSP/CM must manually enter the result for each query by selecting one of the options under the “**Adverse Information on File**” block for each record. Click the

<Save> button located at the left hand side of the NPDB section header to complete the NPDB section of the PSV process.

The screenshot shows the CCQAS Prime Source Verification (PSV) form for PROVIDER49. The form is divided into several sections:

- Health Status:** Contains 7 questions with radio button options for Yes/No and a Comments field.
- Reference:** A table with columns: Current, Name, Title/Position, Address, City, State, Verified.
- NPDB Information:** Includes Last Query Date, Query Results Pending, Request Query, Adverse Information On File (Yes/No/No, but was previously Yes), and Remarks.
- HIPDB Information:** Similar to NPDB Information.
- FSMB Information:** Similar to NPDB Information.

Buttons at the bottom include Print, Complete PSV, Return, and Close. A Save button is located at the top left of the NPDB/HIPDB/FSMB section.

Exhibit 5.7-4. The NPDB/HIPDB Section

The PSV may not be completed until all required credentials have been verified and the results of the NPDB query have been updated on the PSV screen.

Note: Army and Air Force may also perform NPDB queries manually without using the NPDB Batch Query report generated by CCQAS. For manual NPDB queries, Army and AF users should manually enter the Last Query Date and the results of the NPDB query directly into the PSV screen.

Whether the query is done by the batch method or one by one, the result has to be entered manually: one of the buttons in the “Adverse Information on File” block must be selected, and the report has to be uploaded into CCQAS and associated with the provider’s record.

The remaining tabs in the application, Privileges tab, Documents tab, and the Comments tab, are similar in form and function to the tabs described in Sections 5.5.3, 5.5.4, and 5.5.5, respectively.

The CC/MSSP/CM may perform one of several actions using the buttons provided at the bottom of any tab within the application package:

- **<Print>** will send the Provider PSV Summary screen to the printer configured for the user's workstation
- **<Complete PSV>** (see below)
- **<Return>** will route the application back to the CC/MSSP/CM who has ownership of the application; the person in the role (whether CVO or CC/MSSP/CM) performing the PSV is required to enter comments explaining why the application is being returned. The CC/MSSP/CM will then receive a new work list item indicating that the application has been returned without a completed PSV
- **<Close>** will close the application which may then be reopened again later

Following completion of all required PSV, the **<Complete PSV>** button at the bottom of the screen will be enabled. Clicking **<Complete PSV>** has several implications:

- The application will be returned to the CC/MSSP/CM who has ownership of the application
- The application is ready for the CC/MSSP/CM to route it through the review process
- The credentials information entered into the electronic application will be used to create or update the provider's permanent credentials record in CCQAS. If the provider is newly accessed into military service or employment, the application will be used to populate a new credentials record; if the provider already has an active credentials record in CCQAS, the application will be used to update the credentials records already residing in CCQAS

5.8 Primary Source Verification of a Privilege Application by the CVO

The process for PSV by CVO is nearly identical to the process described in Section 5.7. The only difference is that custody of the record is transferred to the UIC associated with the CVO function for the PSV process. Following completion of the PSV, the privilege application is automatically routed back to the CC/MSSP/CM who has ownership of the application.

5.9 Building Workflow for Application Review

Following completion of the PSV, the application is returned to the CC/MSSP/CM for routing through the application review process. If the application was submitted by a CSS member or a provider that is not eligible for privileging, the application will be automatically closed by CCQAS. A read-only version of the application will be permanently stored in the "Applications" tab as part of the provider's historical record.

If the provider is requesting clinical privileges with his/her application, the CC/MSSP/CM may initiate application routing by clicking the **<Routing>** button at the

bottom of the screen within the provider's application (Exhibit 5.9-1). The <Routing> button is only enabled after PSV of the application has been completed.

The screenshot shows the CCQAS (Centralized Credentials Quality Assurance System) interface. The browser title is "CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer". The page header includes the CCQAS logo and the tagline "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness". The main navigation bar contains "Credentialing", "Privileging", "Reports", "System", and "Help".

The current view is "Provider Application Review - PROVIDER71 PROVIDER71_D00000015". Below this, there are tabs for "Provider Summary", "Position", "Privileges", "Documents", and "Comments". A "View Credentials" button is located below the tabs.

The "Profile" section displays the following information:

Name:	PROVIDER71, PROVIDER71	Gender:	Male	Date of Birth:	12/29/1978
Branch:	A11 - Army (USA) Active Duty	Rank:	CPT - Captain	Corps:	MC - Medical Corps
AOC/Design/AFSC:	80H - Cardiologist	ASI:	-	Accession:	DA - Direct Accession

The "Identification" section shows:

Identification Type	Identification Number	State
Social Security Number	D00000015	

The "Contact - Phone" section shows:

Phone Number	Phone Type	Primary
(111) 222-3333	Home	Yes

The "Contact - Email" section shows:

Email Address	Primary
ctest@asmr.com	Yes

The "Contact - Address" section shows: [No Data]

At the bottom of the screen, there are five buttons: "Return to Provider", "Routing", "Re-assign CC/CM/MSSP", "Terminate", and "Close".

Exhibit 5.9-1. The Application Routing Button

The Application Routing screen is returned.

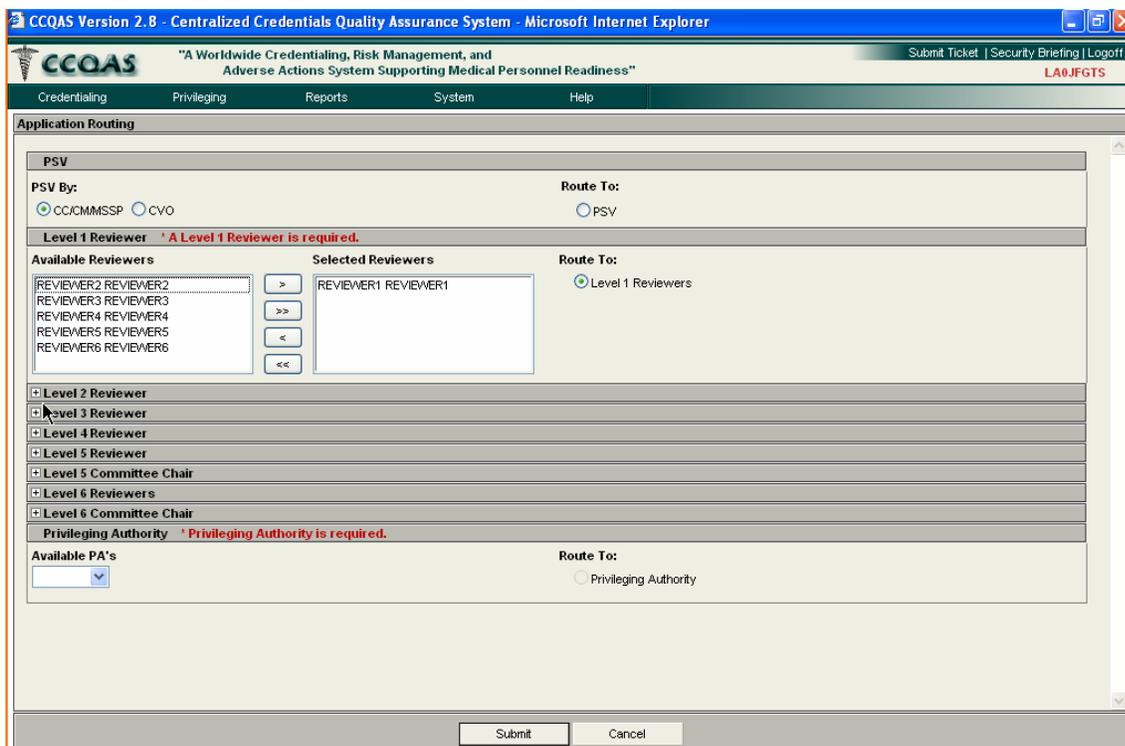


Exhibit 5.9-2. The Application Routing Screen

Important features of the Application Routing screen include:

- Level 1 review and Privileging Authority (PA) review are required by CCQAS for all applications. CCQAS allows optional use of Levels 2 - 6 according to the privileging process for the individual facility or unit
- Levels 2 – 6 may be expanded or collapsed by clicking the [+] or [-], respectively, to the left of the section header
- For each level, the list of all available reviewers associated with the facility or unit will appear in the “**Available Reviewers**” box
- One or more reviewers may be selected at each level by clicking on the desired reviewer’s name and then clicking [>] to move the reviewer’s name to the “**Selected Reviewers**” box. Double-clicking on the name will also move it to the “Selected Reviewers” box.
- A reviewer’s name may be removed from the “**Selected Reviewers**” box by clicking on the desired reviewer’s name and then clicking [<] to move the reviewer’s name back to the “**Available Reviewers**” box. Double-clicking on the name will also move it to the “Available Reviewers” box.
- Clicking [>>] will move all reviewer’s names from the “**Available Reviewers**” box to the “**Selected Reviewers**” box
- Clicking [<<] will move all reviewer’s names from the **Selected Reviewers** box to the “**Available Reviewers**” box
- Levels 5 and 6 are committee levels whereby at least one committee member and one and only one committee chairperson must be selected to participate in the review process

- The names of all individuals that hold PA permissions for the facility or unit will be included in the pick list for “**Available PAs**”.
- An application is routed by selecting the appropriate “**Route To**” radio button, but all routing must be done in chronological order and conclude with the PA review.

The following rules apply to the routing of a privilege application from one level of review to the next:

- Level 1 review should be assigned to the provider’s clinical supervisor; if the provider will have multiple clinical supervisors (as may be the case of providers with more than one specialty), each supervisor should be assigned as a Level 1 reviewer for the application
- An application will not move to the next level until the current level of review has been completed. If multiple reviewers are associated with the current level, all reviewers must complete their review in order for the application to move forward
- If all reviews at the current level take an action of “**Recommend**”, the application will automatically advance to the next level of review without being returned to the CC/MSSP/CM
- If any one reviewer elects to take an action of “**Recommend with Modification**”, “**Do Not Recommend**” or “**Return without Action**”, the application will be returned to the CC/MSSP/CM who will then need to take the appropriate action before submitting the application back into the review process
- Levels 5 and 6, the committee levels, require all committee members to complete their reviews before the committee chair renders the committee’s recommendation
- The final committee recommendation for Levels 5 and 6 reflect the recommendation submitted by the committee chair
- Once workflow routing has commenced, an application may be routed back to a previous level for reconsideration, but the CC/MSSP/CM cannot skip any levels to advance the application forward

The CC/MSSP/CM will select the appropriate reviewers for Level 1, the PA, and other levels deemed necessary for his/her facility’s or unit’s privileging process. The CC/MSSP/CM may simply click on <**Submit**> to initiate routing. Once <**Submit**> is selected, the application is sent to all individuals that were selected as Level 1 reviewers. Each Level 1 reviewer will receive an email notification indicating he/she has a new task in his/her work list that requires action.

5.10 Tracking an Application in Review

Throughout the application review process, the CC/MSSP/CM may view the status of an application at any time without disrupting the workflow process. This may be done from the “My Applications” tab. For applications currently in the review process, the “Application Status = *In Review*” (Exhibit 5.10-1).

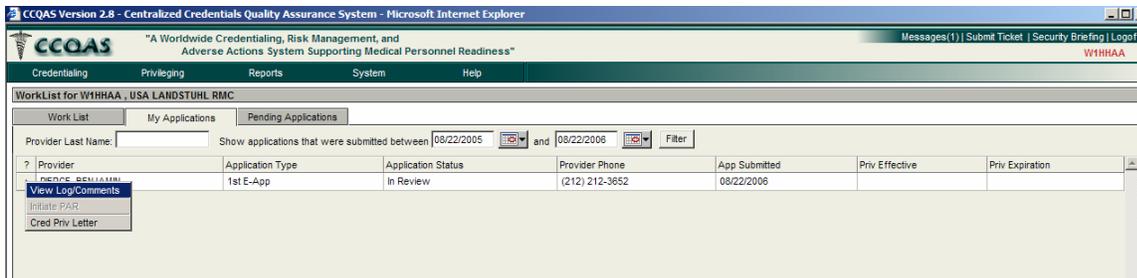


Exhibit 5.10-1. The In Review Status Indicator

A detailed summary of actions performed to date on the application may be viewed by selecting “View Log/Comments” (see Exhibit 5.10-1) from the hidden menu of actions for the application.

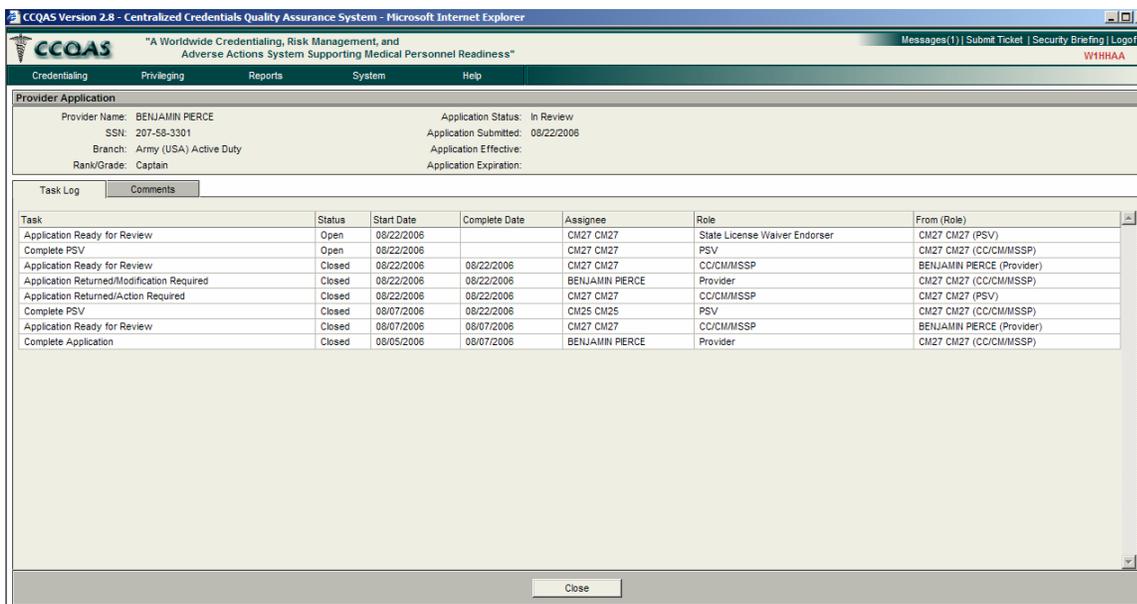


Exhibit 5.10-2. The Task Log Tab

The “Task Log” (Exhibit 5.10-2) displays a summary line for every completed or pending action associated with the privilege application, in order of completion, with the most recent task listed first. Those tasks with “Status = *Closed*” have been completed. Tasks that have no date in the “Complete Date” column are still pending with “Status = *Open*”.

The “Comments” tab (Exhibit 5.10-3) enables the CC/MSSP/CM to view comments and recommendations made by the reviewer who performed each task.

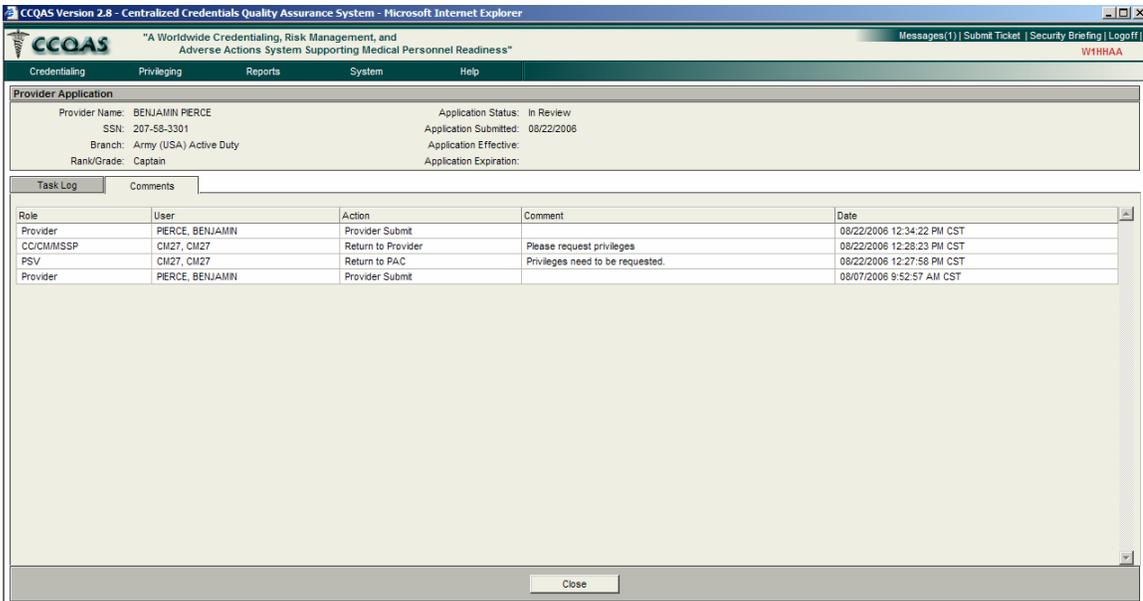


Exhibit 5.10-3. The Comments Tab

Any comments entered into CCQAS during the application review process will be retained on the “Comments” tab as a permanent part of the historical record. The “Comments” tab, however, is not viewable by the provider at any time during or after the review process.

5.11 Pulling an Application Out of the Review Process

The CC/MSSP/CM has the ability to retrieve privilege applications currently in the review process. This may be necessary when an application was inadvertently routed to a reviewer inappropriate for the application, or the assigned reviewer is unable to take necessary action on the application. To pull an application out of the review process, the CC/MSSP/CM selects the individual’s name from the “User” pick list located in the upper right corner of the work list.

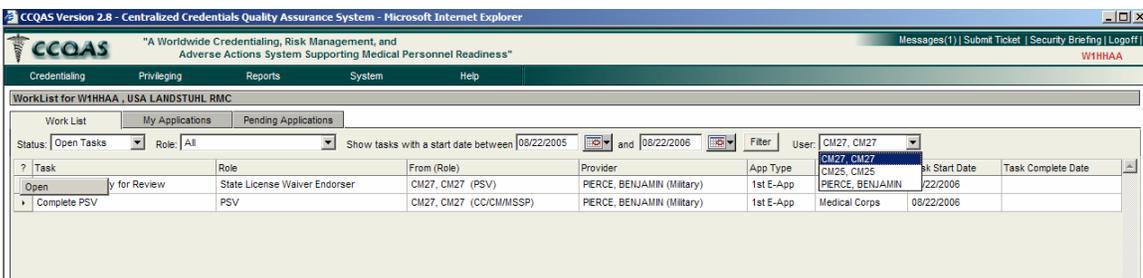


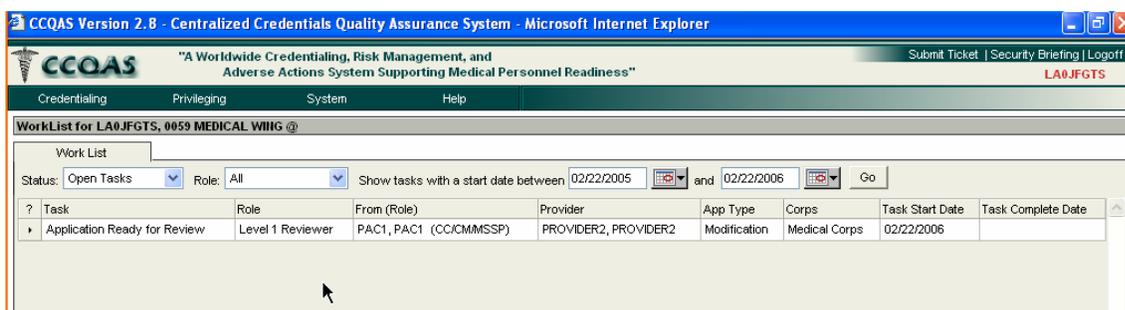
Exhibit 5.11-1. Retrieving an Application in Review

The “User” pick list contains the name of all individuals who have been assigned to take some action on the application. By selecting a user’s name, the CC/MSSP/CM will gain access to that individual’s work list. At that point, the CC/MSSP/CM may select the specific application that needs to be retrieved, open the active work list item associated

with that application, and click the <**Return w/out Action**> button. This action will result in custody of the application going back to the CC/MSSP/CM who originally routed the application for review. The CC/MSSP/CM may then change the assigned reviewers and re-initiate the routing of the application.

5.12 Level 1 Review of an Application

Once a the CC/MSSP/CM routes the application for Level 1 review, each Level 1 reviewer will receive an email notification of a new task in CCQAS and a new task, “Task = *Application Ready for Review*” (Exhibit 5.12-1), will be added to his or her work list. The application may be viewed from the work list by selecting “Open” from the hidden menu, or double-clicking anywhere on the record line.



Task	Role	From (Role)	Provider	App Type	Corps	Task Start Date	Task Complete Date
Application Ready for Review	Level 1 Reviewer	PAC1, PAC1 (CC/MMSSP)	PROVIDER2, PROVIDER2	Modification	Medical Corps	02/22/2006	

Exhibit 5.12-1. The Work List for a Level 1 Reviewer

The electronic privilege application will be returned as a series of tabs. The reviewer will see the same tabs and screens that the CC/MSSP/CM sees during his/her initial review of the application, with a few important exceptions:

- A red flag () will alert the reviewer to any notes entered into the credentials portion of the application (on the “Provider Summary” tab) by the CC/MSSP/CM. The reviewer may view the notes by clicking on the red flag (). The reviewer, however, cannot enter notes into the credentials portion of the application
- All information entered on the Position tab will be read-only for the reviewer
- The Privileges tab contains additional data fields with a pick list (see Exhibit 5.12-2) from which the Level 1 reviewer can select delineations for endorsing each privilege item requested by the provider

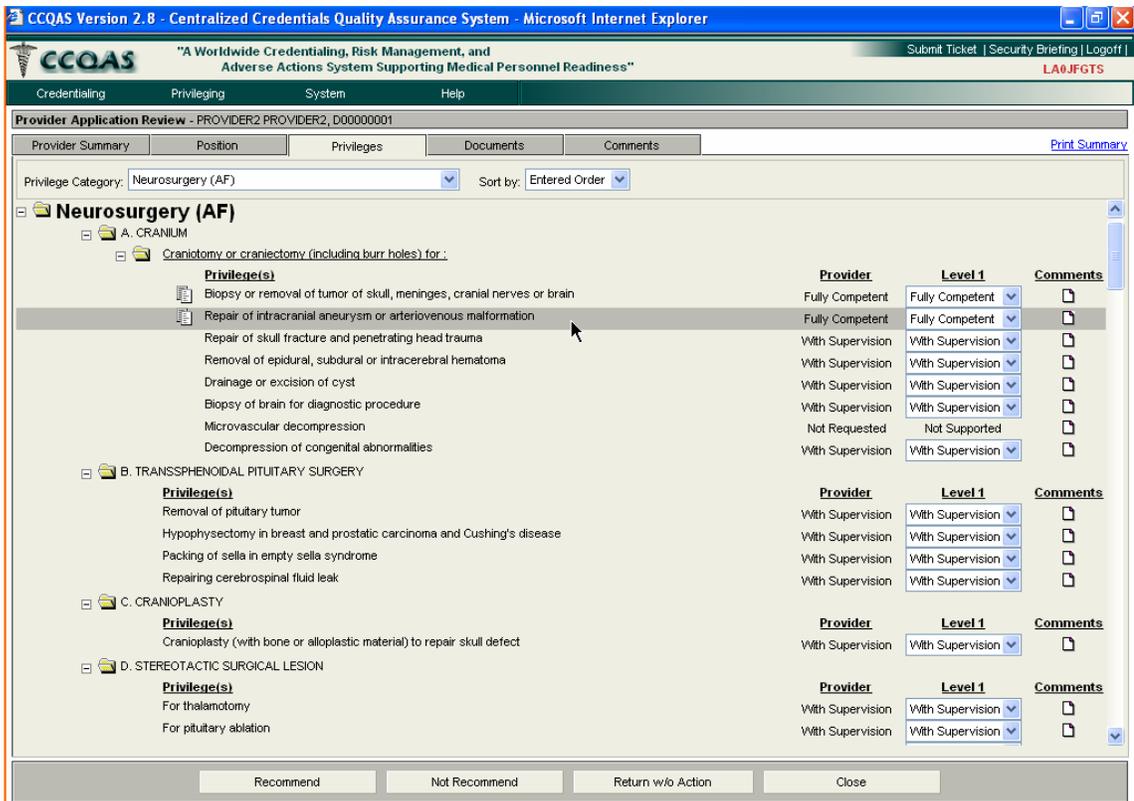


Exhibit 5.12-2. The Privileges Tab for a Level 1 Reviewer

The Level 1 reviewer is required to assign a delineation for each privilege item requested by the provider. If the reviewer elects to assign a privilege delineation that differs from that which the provider requested, the reviewer is required to enter a comment by clicking on the empty notes icon (📝) directly to the right of the delineation, explaining the reason for the difference. Discrepancies between the provider's and the Level 1 reviewer's privilege delineation will also be noted with a red flag (🚩) that will alert subsequent level reviewers of the change.

Note: If a provider has requested privileges in multiple specialties, several Level 1 reviewers will likely be assigned to review the requested privileges. In this situation, each Level 1 reviewer should endorse only the privileges in the specialty that he/she is qualified to review, and leave the remaining privileges for other specialties unchanged from the defaulted value (which is the same as that requested by the provider) for the other Level 1 reviewer to review. Multiple Level 1 reviewers may also endorse the same set of privileges. Each should enter his/her own endorsement and comments, but if the two reviewers differ in their recommendations regarding a particular privilege item, the privilege item will be flagged (🚩) and the privilege delineation field will be blank for subsequent levels of review, and the PA will be required to enter a privilege delineation during the Level 7 review.

After reviewing and assigning privilege delineations, each Level 1 reviewer will then submit his/her overall recommendation for the privilege application by selecting one of the buttons at the bottom of the screen:

- **<Recommend>** indicates that the reviewer recommends approval of the provider's request for privileges with the delineations he/she has entered
- **<Recommend with Modification>** indicates that the reviewer has elected to enter a delineation or delineations that may be different from what the provider has requested, or has entered comments related to individual privileges. If this action is selected, the reviewer is required to enter general comments explaining the reason for his choice of endorsement
- **<Do Not Recommend>** indicates that the reviewer does not support the granting of clinical privileges to the provider, regardless of any changes they may have made on the Privilege tab. If this action is selected, the Reviewer is required to enter comments explaining his/her reason for not recommending the provider for privileges. This option has negative repercussions for the provider and should therefore be selected only after serious, thorough and thoughtful consideration of all factors related to the provider and his application
- **<Return without Action>** will route the application back to the CC/MSSP/CM without a recommendation. If this action is selected, the Reviewer is required to enter comments explaining his/her reason for returning the application. This is usually the appropriate choice if a reviewer, rather than create an *adverse privileging action* with a <Do Not Recommend> action, prefers to return the application to the professional affairs office pending satisfaction of issues regarding the application or with the provider
- **<Close>** will close the application which the reviewer may then reopen at a later time to complete the review

Once the reviewer selects **<Recommend>**, **<Recommend with Modification>**, **<Do Not Recommend>**, or **<Return without Action>**, the application will either be returned to the CC/MSSP/CM or advanced to the next level of review. The reviewer is given an opportunity to enter comments with his/her submission, and comments are required if either **<Recommend with Modification>**, **<Do Not Recommend>** or **<Return without Action>** was selected. All comments entered during the review process became a permanent part of the privileging application.

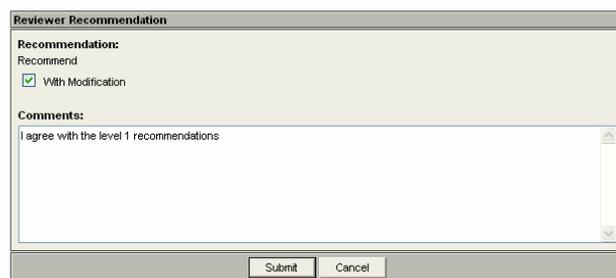


Exhibit 5.12-3. Reviewer Recommendation Screen

Note: Comments entered during the review process will be viewable by the CC/MSSP/CM, other reviewers, and the PA, but the provider will not have visibility of these comments either during or after the processing of their application.

Once an application review task has been completed by a reviewer, the application may be viewed in read-only format from the Application tab. The reviewer, however, may not make further edits to privilege delineations unless the CC/MSSP/CM routes the application back to them for a second review.

After all Level 1 reviewers have completed their reviews, the application may either be routed directly to the next review level in the workflow, or be returned to the CC/MSSP/CM. All Level 1 reviewers must issue a <Recommend> vote on the application for it to advance to the next level of review. If any Level 1 reviewer issues a <Recommend with Modification>, <Do Not Recommend> or <Return without Action> vote, the application will be returned to the CC/MSSP/CM who holds responsibility for the application. In order for an application to advance past Level 1, the underlying issue with the application must be addressed, and then the application must be rerouted through the Level 1 review to obtain a **Recommend** vote from all Level 1 reviewers.

5.13 Levels 2, 3, and 4 Review of an Application

Once an application has cleared the Level 1 review, it will advance to the next level of review assigned to the application. The review process at subsequent levels of review is similar to that described in the previous sections for the Level 1 review with one exception. Levels 2, 3 and 4 reviewers do not have the capability to apply a delineation for individual privilege items in the electronic application, but they do have full visibility of all comments entered into the application by the CC/MSSP/CM, and the privilege delineations and comments entered by the Level 1 reviewer.

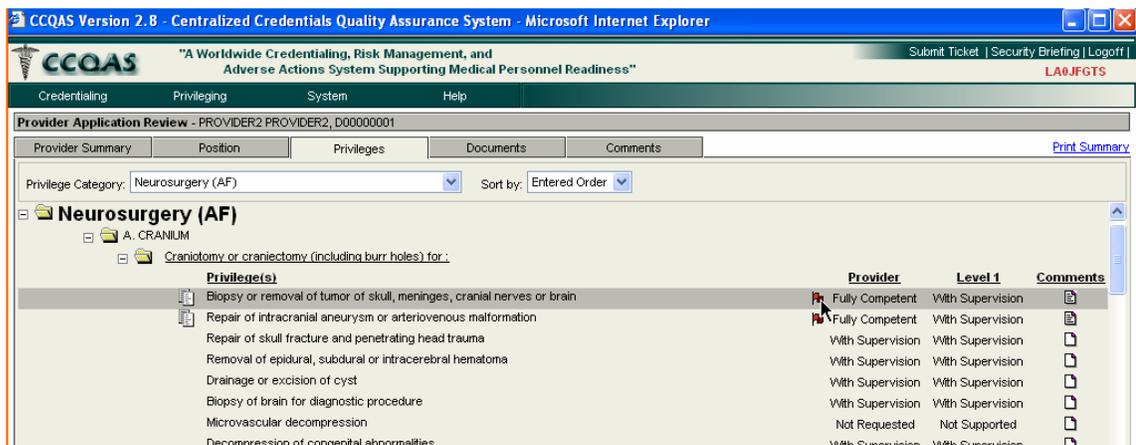


Exhibit 5.13-1. The Privilege Tab for Review Levels 2, 3, and 4

The red flag (🚩) denotes a change made to a privilege delineation by the Level 1 reviewer. Reviewers at subsequent levels of review may click on the (📄) to the right of the privilege item to view the Level 1 reviewer's rationale for changing the privilege delineation.

After reviewing the privilege application and comments left by the previous levels of review, the Level 2, 3, or 4 reviewer submits his/her recommendation by clicking one of the buttons at the bottom of the screen (see Exhibit 5.12-2). All reviewers will be given the opportunity to enter comments with their recommendation, which will then become a permanent part of the privileging application.

5.14 Levels 5 or 6 (Committee) Review of an Application

Levels 5 and 6 in the review process are reserved for committee review of privilege applications. Levels 5 and 6 are comprised of two layers of review within each level to accommodate reviews by each of the committee members, followed by a review by the committee chairperson. Once an application is routed for committee review, each committee member assigned to review the application will receive an email notification and a new task, "Task = *Application Ready for Review*." Once all committee members have performed their review and submitted their individual recommendations, the committee chairperson will receive their email notification and a new work list item to review the application. The committee chair will evaluate the individual recommendations of the committee members, as well as, all previous levels of review, and then submit the final committee recommendation.

The review process at Levels 5 and 6 are similar to that described in the previous section for the Levels 2, 3, and 4 in all other respects. Levels 5 and 6 reviewers do not have the capability to enter a delineation for individual privilege items in the electronic application, but they have full visibility of all comments entered into the application by the CC/MSSP/CM, the privilege delineations assigned by the Level 1 reviewer and his comments, and any other comments entered into the electronic application at Levels 2, 3, and 4. Level 5 or 6 review will be complete after the committee chairs submit their recommendation.

5.15 Review of an Application as the Privileging Authority (PA)

The final review of the application is performed by the PA. PA review is required for all applications. The PA will provide the final determination of whether the application is approved or disapproved and only one PA may be assigned to approve an electronic application.

Once an application is routed for PA review, the PA assigned to review the application will receive an email notification and a new task, "Task = *Application Ready for Review*." Upon opening the task, the application will be displayed (Exhibit 5.15-1).

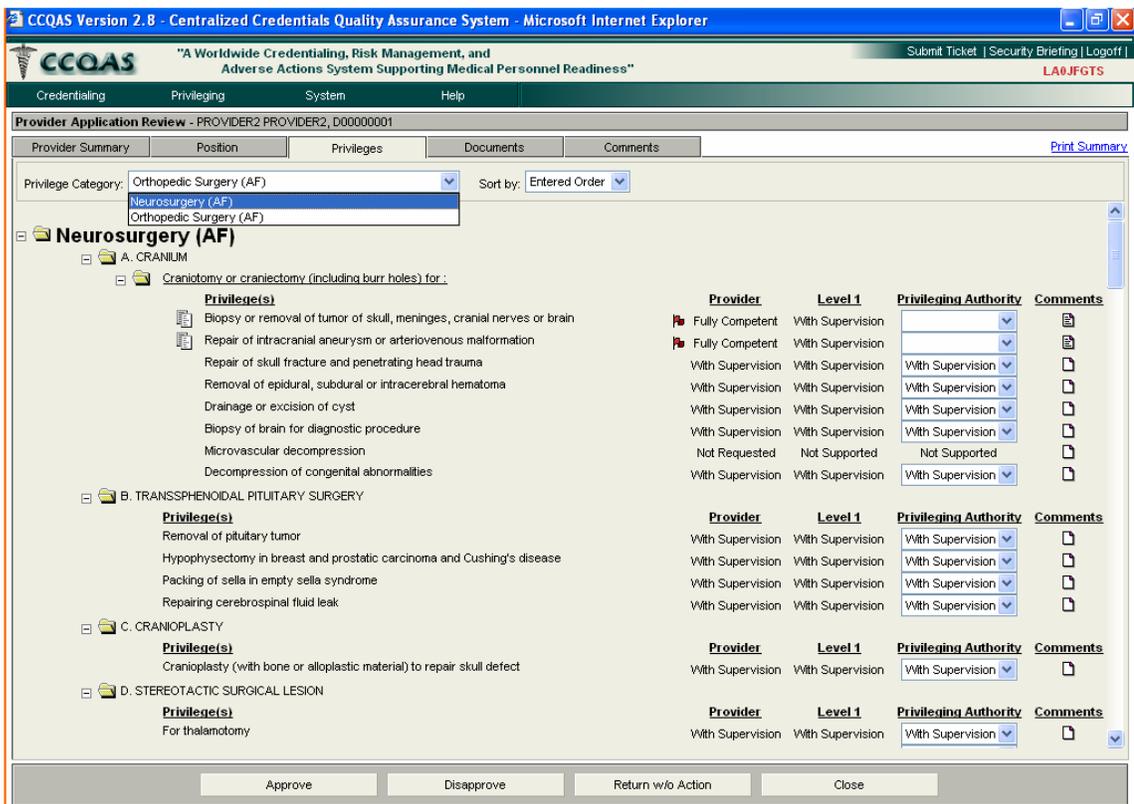


Exhibit 5.15-1. The Privilege Tab for Privileging Authority Review

The PA will see the same tabs and screens that the previous reviewers saw during their review of the application, with a few important differences:

- The Privileges tab contains additional data fields with a drop-down pick list of delineations for the PA's use in endorsing each privilege item requested by the provider
- The PA will submit final approval/disapproval of the application

The PA is required to assign a delineation for each privilege item requested by the provider; however, for his convenience, the delineations are already defaulted to those entered by the Level 1 reviewer, and depending on the recommendations of all the reviewers, he may or may not have to change them. When a delineation field is blank and flagged (resulting from a difference in delineation entered by one or more Level 1 reviewers), the PA has to enter a value which resolves the difference in delineation entered by more than one Level 1 reviewers. As is the case with the Level 1 reviewer, if the PA elects to assign a privilege delineation that differs from that which the provider requested, the PA is required to enter a comment, by clicking on the note icon (📝) directly to the right of his/her delineation, explaining the reason for the difference. Discrepancies between the provider's and the PA's privilege delineation will also be noted with a red flag (🚩).

Note: The PA may either select a set of privileges from the Privilege Category pick list or scroll continuously through the Privileges tab to review all privileges from all categories.

The PA has full visibility of all the reviewers’ recommendations and comments entered into the application during the review process. Comments pertaining to specific privilege items may be viewed by clicking on the filled note icon (📝) next to the privilege item. A summary of recommendations and detailed, application-level comments entered during prior levels of review are summarized on the Comments tab (Exhibit 5.15-2).

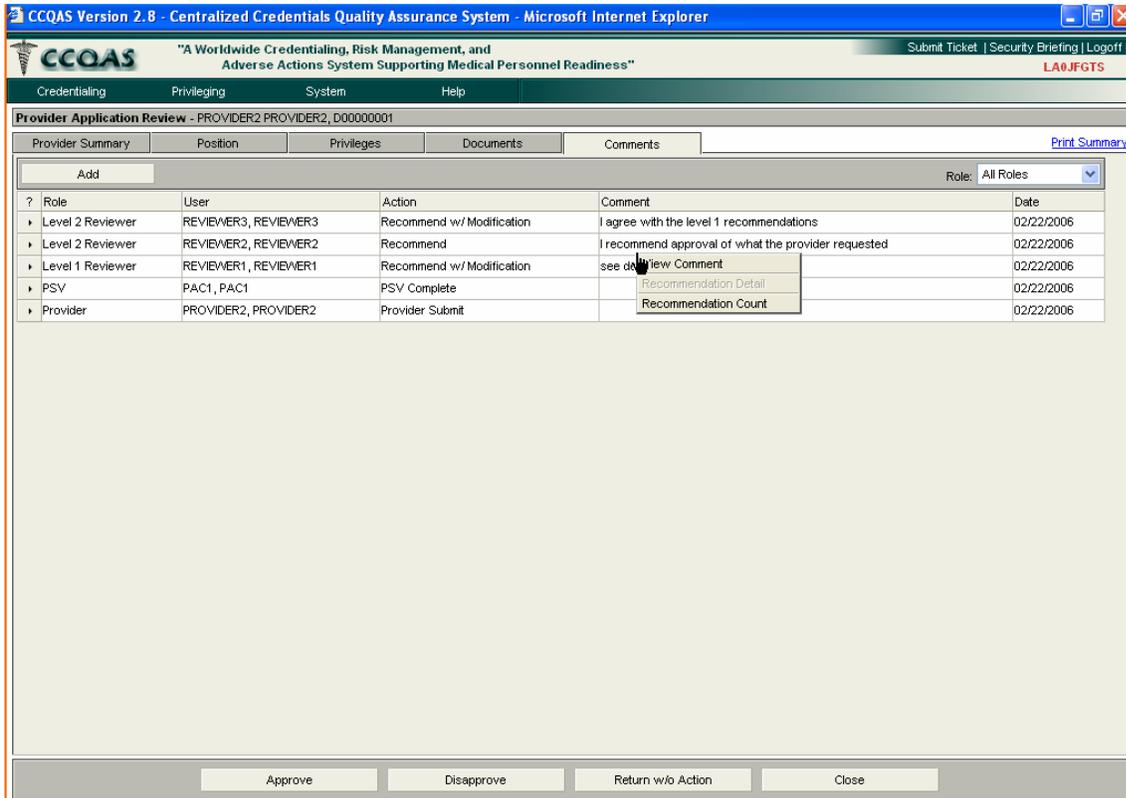


Exhibit 5.15-2. The Comments Tab for PA Review

The “Comments” tab displays all application-level comments made during the review process in summary form. Detailed comments (Exhibit 5.15-3) entered for individual privilege items may then be viewed by selecting “View Comment” from the hidden menu of actions.

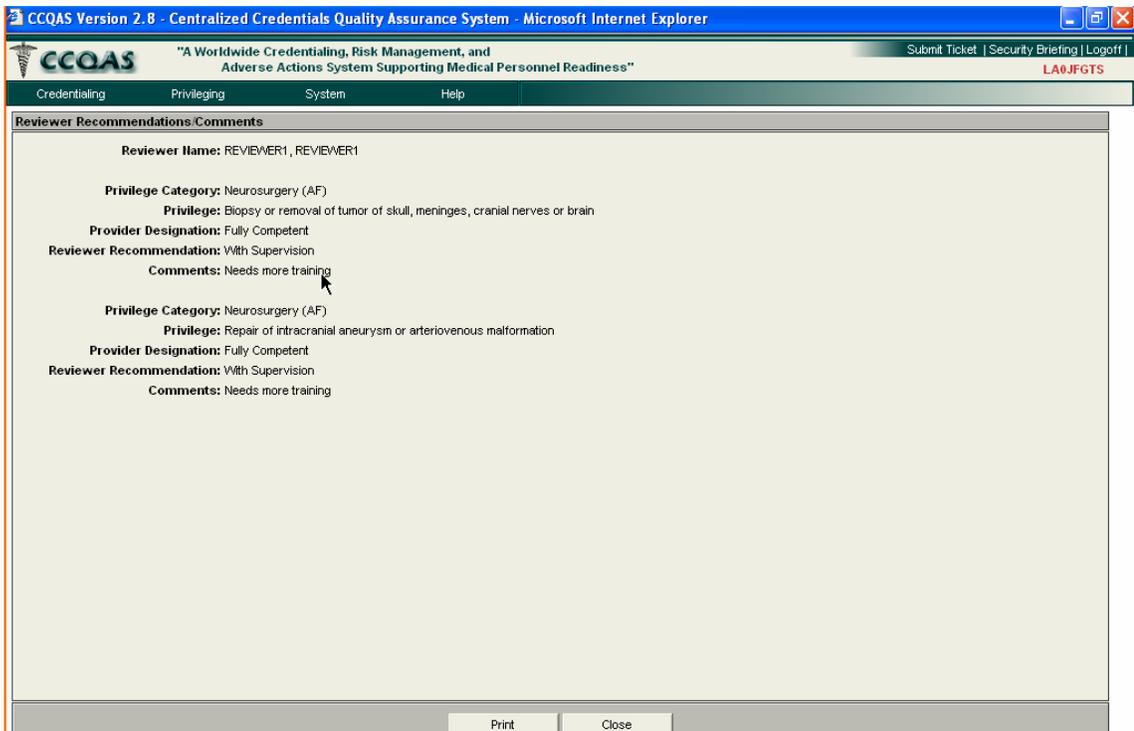


Exhibit 5.15-3. The Reviewer Recommendations/Comments Screen

An inventory of all recommendations (Exhibit 5.15-4) issued during the review process may be viewed by clicking “Recommendation Count” (see Exhibit 5.15-2) from the hidden menu of actions on the “Comments” tab.

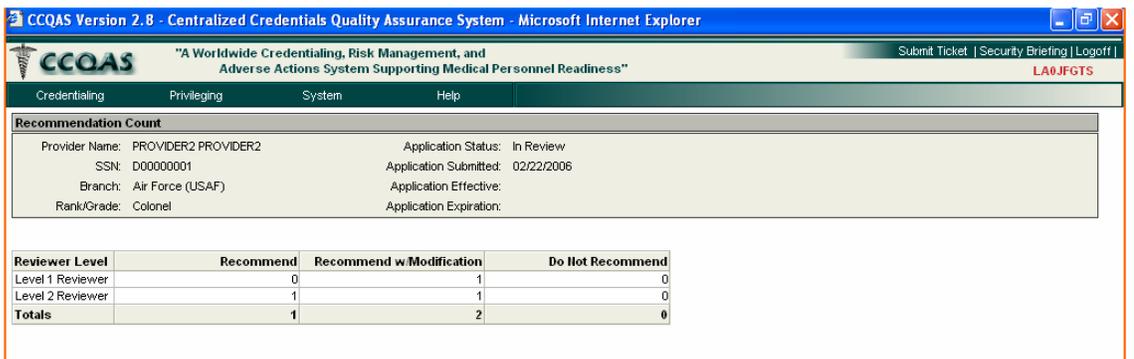


Exhibit 5.15-4. The Recommendations Count Screen

After reviewing the privilege application, recommendations, and comments from previous levels of review, the PA submits his decision by clicking one of the buttons at the bottom of the screen:

- **<Approve>** if the PA wants to approve the provider’s request for privileges with no changes to the delineations as indicated on the Privileges tab, this button should be selected
- **<Approve with Modification>** should be selected if the PA changed a delineation or may have entered comments pertinent to a specific privilege. If this action is selected, the PA is required to enter a general, application-level comment

- **<Disapprove>** should be selected if the PA wants to disapprove the provider's application for clinical privileges, regardless of any changes that may have been made on the Privileges tab. If this action is selected, the PA is required to enter comments explaining his/her reason for not approving the provider for privileges
- **<Return without Action>** will return the application to the CC/MSSP/CM without any approval action by the PA. If this action is selected, the PA is required to enter comments explaining his/her reason for returning the application
- **<Close>** will close the application which the PA may then reopen at a later time to complete the review

Since the PA is the last level in the review process, regardless of which action he selects, the application will be routed back to the CC/MSSP/CM. The only action that may require rerouting of the application back to the PA is **<Return without Action>**. The PA is given an opportunity to enter comments with his/her submission, and comments are required if **<Approve with Modification>**, **<Disapprove>** or **<Return without Action>** are selected. All comments entered by the PA during the review process become a permanent part of the privileging application.

Exhibit 5.15-5. The Privileging Authority Decision Screen

Note: Comments entered during the review process will be viewable by the CC/MSSP/CM and other reviewers but the provider will not have visibility of these comments either during or after the application review process.

Once an application has been returned to the CC/MSSP/CM, the PA continues to have access to the application in read-only format from the Application tab. The PA, however, cannot make further edits to privilege delineations unless the CC/MSSP/CM routes the application back to him/her for a second review.

5.16 Completing the Application Approval Process

Once the PA submits his/her final decision to approve the application for clinical privileges, the application is routed back to the owning CC/MSSP/CM. The CC/MSSP/CM will complete the approval process by routing approval notifications to the provider, Level 1 reviewers, and other individuals involved in the review process that should be notified. The notification process is initiated by selecting **<Notifications>** at the bottom of the screen (Exhibit 5.16-1).

Note: The automated notification functionality in CCQAS should be used in cases where the provider’s application for clinical privileges is approved by the PA. In situations where the PA disapproves a provider’s application, communications with the provider should be handled outside CCQAS and Service and MTF protocols should be followed.

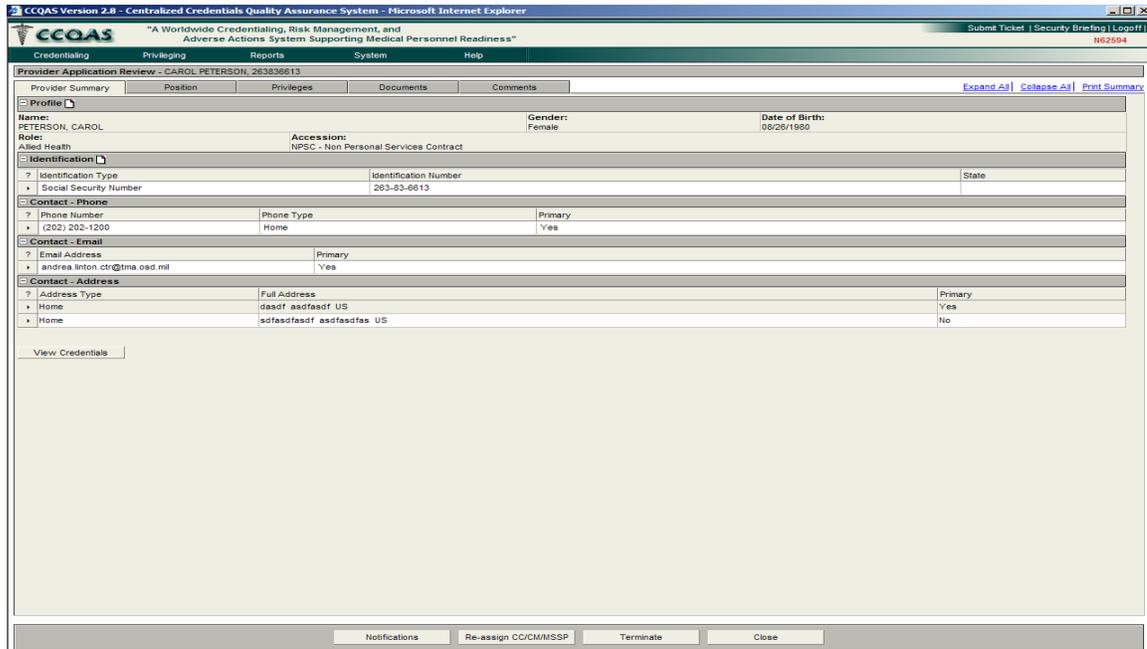


Exhibit 5.16-1. The Notification Routing Button

The “Notification Routing” screen will be returned.

Exhibit 5.16-2. The Notification Routing Screen

Important features of the “Notification Routing” screen include:

- The CC/MSSP/CM is required to select the appropriate radio button for “**Notify Provider**”, but notification at other review levels are not required by CCQAS
- If “**Notify Provider = Yes**” is selected, the CC/MSSP/CM is required to enter the number of days the provider acknowledgment is due
- Levels 2 – 6 may be expanded or collapsed by clicking the [+] or [-], respectively, to the left of the section header
- For each level, the list of all reviewers will appear in the “**Available Reviewers**” box
- One or more reviewers may be selected at each level, but clicking on the desired reviewer’s name and then clicking [>] to move the reviewer’s name to the “**Selected Reviewers**” box. Double-clicking on the name will also move it to the “Selected Reviewers” box
- A reviewer’s name may be removed from the “**Selected Reviewers**” box by clicking on the desired reviewer’s name and then clicking [<] to move the reviewer’s name back to the “**Available Reviewers**” box. Double-clicking on the name will also move it back to the “Available Reviewers” box
- Clicking [>>] will move all reviewer’s names from the “**Available Reviewers**” box to the “**Selected Reviewers**” box.
- Clicking [<<] will move all reviewer’s names from the “**Selected Reviewers**” box to the “**Available Reviewers**” box.

After the CC/MSSP/CM selects the desired recipients for the approval notification, he/she clicks <**Submit**>. A notification email will then be distributed to all recipients simultaneously. If the provider is required to acknowledge the approved application,

he/she will receive a new work list item with “Task = *Privileging Notification*”, as well as, the email notification. Providers should acknowledge the award of privileges within the specified number of days. Reviewers are not required to acknowledge the approved application and will receive only an email notification. They are not required to take any further action regarding the application.

When a provider receives a new work list item with “Task = *Privileging Notification*” he/she may acknowledge the approved application by first opening the task. At the top of the “Provider Summary” tab is a statement as to the type of appointment and privileges the provider has been granted, and instructions on acknowledging the appointment.

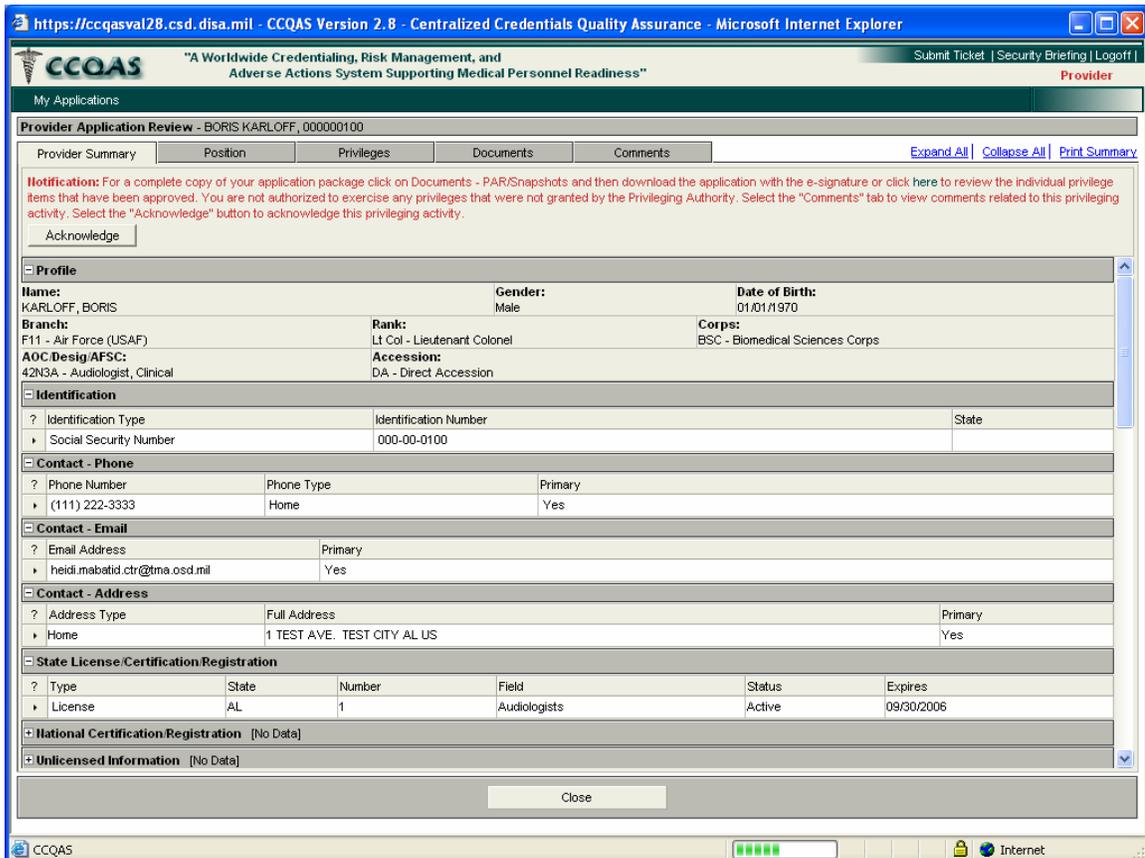


Exhibit 5.16-3. Provider <Acknowledge> Button on Summary Page

When the provider clicks the <Acknowledge> button, a page with all the statements regarding duties and responsibilities, and compliance with Service/MTF regulations and staff by-laws is returned.

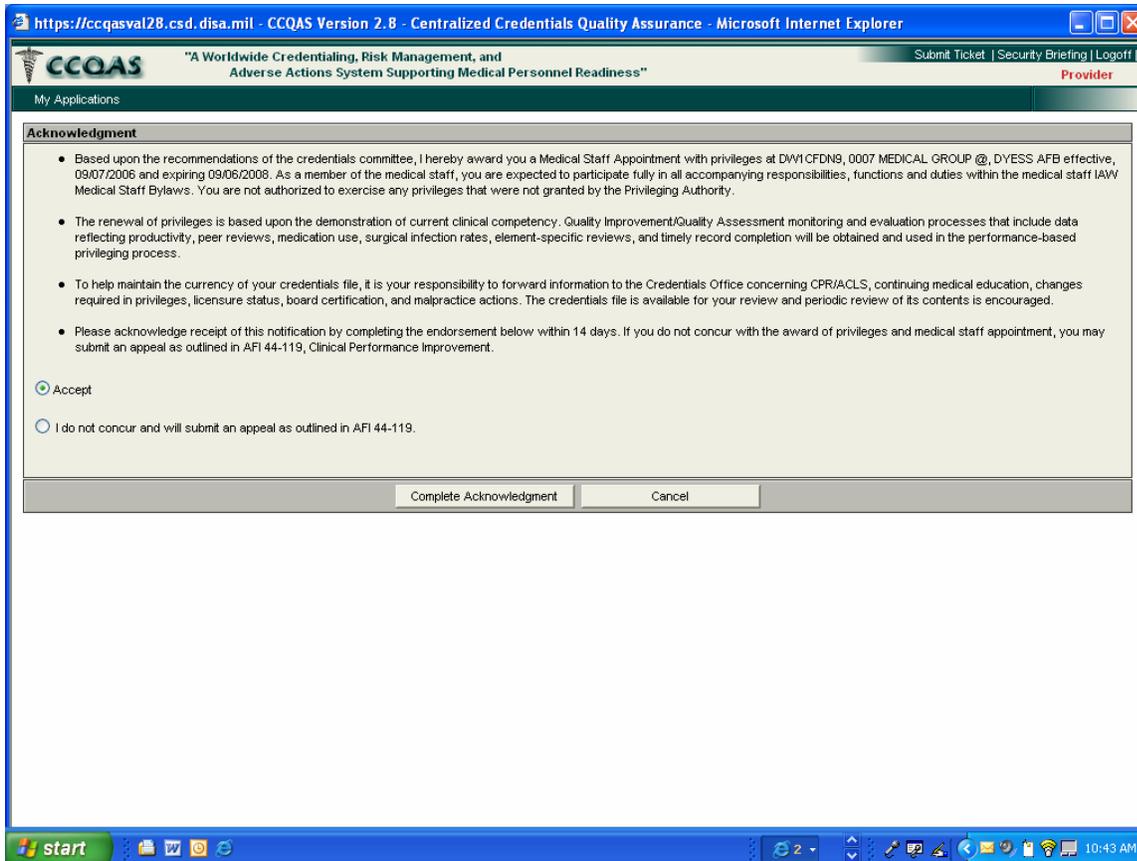


Exhibit 15.6-4. Provider “Complete Acknowledgment” Page

The provider has to choose <I accept>, or <I do not accept>. The acknowledgment is then returned to the CC/MSSP/CM in the form of a new work list item with “Task = *Privileging Acknowledgment Received*”. When the work list item is opened, the provider acknowledgment will be visible at the top of the Provider Summary page that is returned.



Exhibit 5.16-5. The Complete Button

The CC/MSSP/CM may then click the <Complete> button; this action ends the automated processing of the privilege application, regardless of whether the provider chooses to accept or not accept the awarded privileges. If the provider chooses not to accept the Privileging Authority’s decision and wants to submit an appeal, the appeal process is handled outside of the system.

Following the CC/MSSP/CM's clicking of the <Complete> button, the application review process is closed. The CC/MSSP/CM, the PA, the reviewers and the provider may access a read-only version of the approved application from the "Applications" tab at any time.

5.17 The Updated Provider Credentials Record

The credentials information entered into the electronic application is used to create or update the provider's permanent credentials record in CCQAS. If the provider is newly accessed into military service or employment, the application will be used to create a new credentials record. For a provider that already has an active credentials record in CCQAS at the time the PSV was completed, the application will be used to update the credentials record already residing in CCQAS.

The credentials data from the application will be imported into the Credentialing module of CCQAS after the PSV of the application has been completed. The credentials record is then available to any credentials staff member that has permission to access the Credentialing module for his/her unit for updates, reports and/or generation of pre-formatted letters.

The "Privileges" section (Exhibit 5.17-1) of the provider's credentials record will reflect the privileges that were awarded with the approved application. The "Privileges" section should contain a summary record line for each privilege application that was approved.

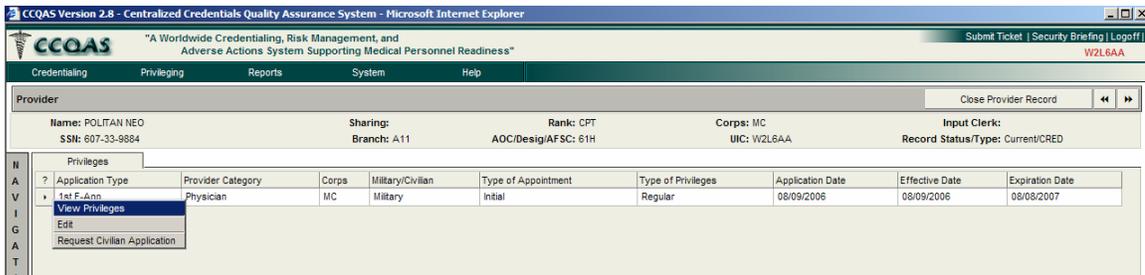


Exhibit 5.17-1. The Privileges Tab in the Credentials Record

To see the approved privileges, select "View Privileges" from the hidden menu of actions for the privilege application.

CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"

Submit Ticket | Security Briefing | Logout | W2L6AA

Credentialing Privileging Reports System Help

PRIVILEGED PROVIDER INFORMATION REPORT

SERVICE: ARMY
UIC: W2L6AA MTF: WOMACK ARMY MED CTR

PROVIDER	SSN	MILITARY/CIVILIAN	TYPE OF PRIVILEGES
NEO, POLITAN	607-33-9884	Military	Regular

PRIVILEGE CATEGORY: Family Practice (A)
Category I. Emergency Care. Uncomplicated illnesses or problems which have low risk to the patient such as routine prenatal health care, incision and evacuation of thrombosed hemorrhoids, and acute and chronic outpatient care in clinics and emergency services. Residency training is not required but reasonable experience in the care of patients with these problems or in the performance of these procedures is required.

PRIVILEGE ITEM (S)	REQUESTED	APPROVED
Category I clinical privileges	Fully Competent	Fully Competent
Anoscopy	Fully Competent	Fully Competent
ECG performance and initial interpretation	Fully Competent	Fully Competent
Basic radiographical films (skull, spine, chest, abdomen and extremities)	Fully Competent	Fully Competent
Insertion of intrauterine device (IUD)	Fully Competent	Fully Competent
Remove Intrauterine device (IUD)	Fully Competent	Fully Competent
Regional Anesthesia	Fully Competent	Fully Competent
Splinting/Casting/Immobilizing of simple fractures/sprains	Fully Competent	Fully Competent

Close Print

Exhibit 5.17-2. The Privileges Provider Information Report

The list of approved privileges may be printed by clicking <**Print**>. The user will be returned to the Privileges tab by clicking <**Close**>.

Based on the privilege approval date, CCQAS will automatically calculate the privilege expiration date for one year for initial appointments, or for two years for regular appointments. These expiration dates may be edited on the “Privileges” tab by first selecting “Edit” from the hidden menu of actions for the application.

CCQAS Version 2.8 - Centralized Credentials Quality Assurance System - Microsoft Internet Explorer

CCQAS "A Worldwide Credentialing, Risk Management, and Adverse Actions System Supporting Medical Personnel Readiness"

Submit Ticket | Security Briefing | Logout | W2L6AA

Credentialing Privileging Reports System Help

Provider Name: POLITAN NEO SSN: 607-33-9884 Sharing: Branch: A11 Rank: CPT AOC/Desig/AFSC: 61H Corps: MC UIC: W2L6AA Input Clerk: Record Status/Type: Current/CRED

Provider Position

Provider Category: Physician

Duty Section:

Duty Phone:

Rotation/Permanent Change of Station Date:

Date Reported to Current Assignment: 07/01/2006

Type of Privileges Requested: Regular

Privilege Expiration Date: 08/08/2007

Type of Appointment Requested: Initial

Request Admitting Privileges: Yes No

Patients in Age Groups being treated? Check All

- Neonates(Birth-28 days)
- Infants(1-24 months)
- Children(2-12 years)
- Adolescents(13-17 years)
- Young Adults(18-23 years)
- Adults(24-65 years)
- Geriatrics(>65 years)

Save Close

Exhibit 5.17-3. Editing the Privilege Expiration Date on the Position Screen

The “Provider Position” page will then be returned. In prior versions of CCQAS, the **Privilege Expiration Date** and **Staff Appointment Date** were updated on the “Assignments” section of the credentials record. These fields are now read-only in the

“Assignments” section and reflect those dates entered on the “Privileges” tab. The **CSS Review Date** will remain active in the “Assignments” section since CSS members are not eligible for privileging. The expiration dates entered on the Position screen will also dictate when the renewal notices are generated, according to the time period entered on the “Command Parameters” screen (see Section 10).

Note: The “Privileges” tab will only be active or visible for providers who are eligible for privileging. There will be no “Privileges” tab in credentials for clinical support staff or non-privileged providers.

5.18 Frequently Asked Questions

FAQ: I have many privileged providers working at my facility who are in the middle of their biannual privileging cycle. When should these providers be incorporated into the CCQAS 2.8 online privileging process?

Answer: Once CCQAS 2.8 is deployed at your facility, all applications for clinical privileges, including new, modification, and renewal applications, should be submitted electronically through CCQAS 2.8. Using this method, providers will be introduced to the online application process at the time when they would normally start working on their next paper privilege application.

FAQ: I am a credentials staff member who uses CCQAS everyday. Since I check my work list frequently as part of my daily activities, I do not need the email notifications that are filling up my email inbox. Is there any way I can turn my email notifications off?

Answer: Yes, the notification feature may be turned off for any CCQAS user assigned to the CC/MSSP/CM role by clicking on the System main menu, and selecting “Messaging”, then “Email Notifications”. Then follow the instructions on the screen.

This page intentionally left blank.