



HELPING YOUR ORGANIZATION STAY CONNECTED, CURRENT AND READY

CGA Playbook

Providing Carrier Group Administrators (CGAs) with practical guidance for managing user access, maintaining organizational information, supporting colleagues, and fulfilling key responsibilities throughout the year.



TRUSTED | ESSENTIAL | OBJECTIVE

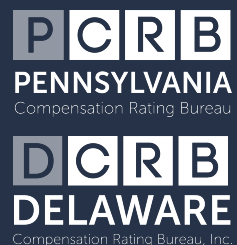


Table of Contents

1. Welcome
2. Why the Carrier Group Administrator Role Matters
3. Understanding Application Manager
4. Understanding Accounts, User Profiles & Access
5. Core Responsibilities
6. Making Access Decisions
7. Managing the User Lifecycle
8. Best Practices
9. Common Scenarios
10. Annual Responsibilities
11. Resources
12. Frequently Asked Questions
13. Annual Checklist



CGA Playbook

September, 2026

Pennsylvania Compensation Rating Bureau (PCRB)

Delaware Compensation Rating Bureau Inc. (DCRB)

30 South 17th Street, Suite 1500

Philadelphia, PA 19003

215-568-2371 / 302-654-1435

www.pcrb.com / www.dcrb.com

This work is protected by copyright. Its use outside of the restricted limits of the copyright law is not permitted without the approval of the publisher and is a punishable offense. This particularly applies to the copying, translating, microfilming, as well as saving and processing in electronic systems. All rights reserved.

1. Welcome

Welcome to Your Role as a Carrier Group Administrator

Congratulations on being designated as a **Carrier Group Administrator (CGA)**.

As a CGA, you serve an important role within your organization by helping ensure employees have timely, appropriate, and secure access to PCRB/DCRB applications and services. Every day, carrier employees rely on these applications to report data, analyze information, manage financial transactions, and perform other essential business functions. Your work helps make those activities possible.

Although much of the role involves Application Manager, the responsibilities extend well beyond administering software. Carrier Group Administrators help protect organizational information, support operational continuity, facilitate communication between their organization and PCRB/DCRB, and ensure application access reflects current business responsibilities.

As PCRB/DCRB continues expanding its digital services, the CGA role will continue growing in importance. By following the guidance in this playbook and using the supporting Application Manager documentation, you'll help your organization maintain secure, efficient, and reliable access to the tools it depends upon.

Purpose of This Playbook

This playbook is designed to help Carrier Group Administrators understand their role and successfully manage Application Manager access throughout the year.

Rather than providing detailed software instructions, this guide focuses on:

- Understanding your responsibilities
- Managing organizational access
- Applying recommended practices
- Making informed access decisions
- Supporting your colleagues
- Maintaining secure operations

Detailed procedures for completing tasks within Application Manager are available in the Application Manager User Guide.

How to Use This Playbook

This guide is organized around the responsibilities of a Carrier Group Administrator.

If you're new to the role, we recommend reading the guide from beginning to end.

Experienced CGAs may prefer to use individual chapters as references when questions arise or when completing annual reviews of user access.



2. Why the CGA Role Matters

More Than an Application Administrator

At first glance, the Carrier Group Administrator role may appear to focus primarily on approving user access requests within Application Manager.

In reality, the role plays a much broader part in helping member carriers interact securely and efficiently with PCRB/DCRB.

Every application a user accesses—and every permission they receive—supports a business purpose. Whether an employee is reporting policy information, reviewing experience modifications, analyzing data, managing invoices, or accessing other PCRB/DCRB services, someone within the organization must help ensure that access is appropriate.

That responsibility belongs to the Carrier Group Administrator.

Supporting Your Organization

Carrier Group Administrators help their organizations:

- Provide employees with timely access to the applications they need.
- Protect confidential carrier information.
- Reduce delays caused by missing or outdated permissions.
- Maintain accurate organizational information.
- Support efficient communication with PCRB/DCRB.
- Promote operational continuity during staffing changes.

These responsibilities contribute directly to your organization's ability to conduct business efficiently.

Supporting PCRB/DCRB

Carrier Group Administrators also support PCRB/DCRB by helping maintain the integrity of Application Manager. Accurate user information, timely permission updates, and appropriate approval decisions all contribute to a more secure and reliable environment for every member carrier.

A Trusted Organizational Role

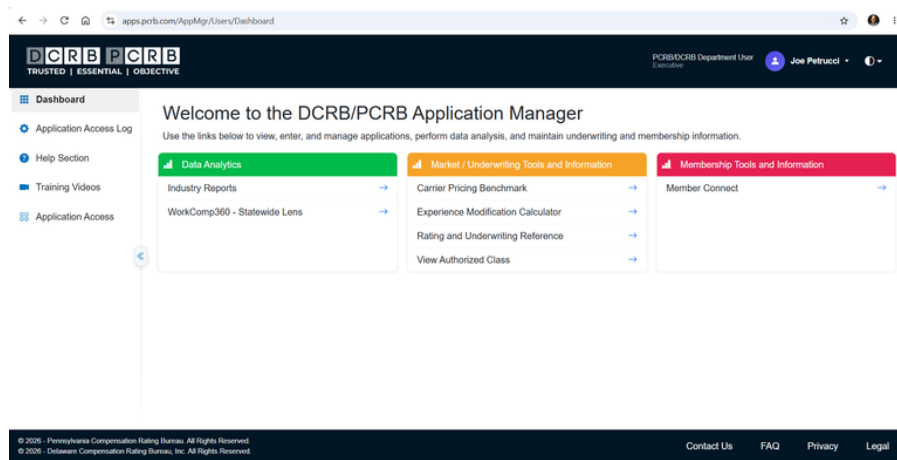
Carrier Group Administrators should be viewed as trusted operational representatives.

Rather than simply administering software, CGAs help manage one of the organization's most important operational resources—secure access to PCRB/DCRB applications and services.

The CGA Commitment

As a Carrier Group Administrator, you have been entrusted with helping your organization maintain secure, efficient access to PCRB/DCRB applications and services. The decisions you make support your colleagues, protect organizational information, and help ensure the right people have the right access at the right time.

3. Understanding Application Manager



Application Manager
is available at
apps.pcrb.com/AppMgr

The Gateway to PCRB/DCRB Digital Services

Application Manager serves as the secure gateway to PCRB/DCRB online applications and services. Instead of maintaining separate usernames and passwords for individual applications, users create a single Application Manager account that allows them to access the applications appropriate for their role.

Application Manager simplifies account management while helping maintain the security of PCRB/DCRB systems and member information.

Why Application Manager Exists

Application Manager was developed to provide:

- One secure sign-in for PCRB/DCRB applications.
- Consistent user authentication.
- Role-based access management.
- Organizational oversight of user permissions.
- Secure administration of carrier access.

Carrier Group Administrators are an essential part of this model because they help ensure user access reflects legitimate business needs.

Your Role Within Application Manager

As a Carrier Group Administrator, you are responsible for managing access—not managing the applications themselves.

Application owners determine how their applications function.

Carrier Group Administrators help determine who may access those applications on behalf of their organization.

Understanding Role-Based Access

Application Manager uses role-based permissions.

Not every user requires access to every application.

Instead, users receive access based on:

- their organization,
- their responsibilities,
- and the applications necessary to perform their work.

This approach strengthens security while ensuring users have the resources they need.

4. Understanding Accounts, User Profiles & Access

Understanding the Building Blocks

Before reviewing access requests, it's important to understand how Application Manager organizes users and permissions.

Although these concepts work together, each serves a different purpose.

Understanding the distinction helps Carrier Group Administrators make informed decisions and answer common user questions.



Accounts

An Application Manager account is an individual's secure login. Each user creates one account using their email address and authentication credentials. The account confirms the user's identity and allows them to access Application Manager. Think of the account as the "front door."

User Profiles

A User Profile connects an individual's account to a specific organization and user type. The profile identifies:

- who the user represents,
- what type of organization they belong to,
- and which applications may be available.

Some individuals maintain multiple user profiles because they perform different roles or represent multiple organizations.

As a Carrier Group Administrator, you'll frequently review requests associated with user profiles rather than user accounts.

Carrier Access

Carrier Access associates a user profile with your member carrier organization. Without Carrier Access, users cannot perform work on behalf of your organization, even if they have an Application Manager account.

Carrier Access should be granted only when a legitimate business need exists.

Application Access

Application Access determines which PCRB/DCRB applications a user may access. Not every user requires every application.

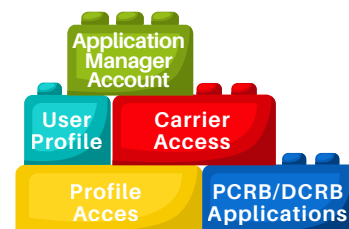
As a Carrier Group Administrator, one of your most important responsibilities is ensuring requested applications align with the user's job responsibilities.

Application access should always reflect business need—not convenience.

Putting It All Together

A helpful way to think about Application Manager is as a series of connected building blocks.

Each layer builds upon the previous one. Understanding this structure will make it much easier to evaluate access requests and assist users throughout the year.



5. Core Responsibilities

Your Core Responsibilities

Now that you understand how Application Manager organizes users and access, it's time to focus on your role as a Carrier Group Administrator.

Although many CGAs spend only a small portion of their day working in Application Manager, the decisions they make help ensure employees have timely access to the PCRB/DCRB applications they need while maintaining appropriate security for their organization.

Your responsibilities generally fall into five areas:



1. Review Access Requests

One of your primary responsibilities is reviewing requests submitted through Application Manager.

Every request should be evaluated to determine whether the requested access is appropriate for the individual's responsibilities.

When reviewing requests, consider:

- Does the user represent your organization?
- Does the requested application support their job responsibilities?
- Does the requested level of access appear appropriate?
- Is additional clarification needed before approval?

Timely review of access requests helps employees begin using PCRB/DCRB applications without unnecessary delays.



2. Maintain User Access

Application access should evolve as responsibilities change.

Employees may:

- move to new departments,
- assume different responsibilities,
- require additional applications,
- no longer require existing applications.

Carrier Group Administrators help ensure Application Manager accurately reflects these changes.

Maintaining current permissions helps improve both security and operational efficiency.



3. Maintain Organizational Access

Carrier Group Administrators also help manage access at the organizational level.

This includes helping ensure:

- appropriate employees have access,
- organizational information remains current,
- Application Manager continues supporting day-to-day business operations.

As organizations grow and change, Application Manager should continue reflecting current organizational needs.



4. Support Organizational Security

Application Manager helps protect PCRB/DCRB systems through secure authentication and role-based access.

Carrier Group Administrators strengthen this security by ensuring:

- users receive only the applications they require,
- unnecessary access is removed,
- permissions remain aligned with current responsibilities,
- former employees no longer retain access.

Strong access management helps reduce organizational risk while protecting confidential carrier information.



5. Support Your Colleagues

Carrier Group Administrators often become the first point of contact for Application Manager questions.

Although Central Support remains available to assist users, many questions can be answered internally by a knowledgeable Carrier Group Administrator.

Examples include:

- Who approves my request?
- Why can't I access an application?
- Do I need another profile?
- Which applications should I request?

Helping colleagues navigate these questions contributes to a better overall member experience.

6. Making Access Decisions

Utilizing Sound Judgement

Perhaps the most important responsibility of a Carrier Group Administrator is determining whether requested access is appropriate.

Application Manager provides the tools to approve requests.

Good judgment ensures those tools are used effectively.

Start With Business Need

Every approval should begin with one question:

Does this individual require this application to perform their responsibilities?

If the answer is yes, the request may be appropriate.

If additional clarification is needed, seek that information before approving the request.

Application access should always support legitimate business activities.



Think Beyond Today

It's natural to focus on an employee's immediate needs.

However, Carrier Group Administrators should also consider whether requested access is appropriate over the long term.

For example:

- Will this responsibility continue?
- Is this temporary access?
- Would another employee be better suited for the application?

Thinking beyond immediate needs helps reduce unnecessary permissions over time.

Follow Organizational Practices

Every organization has its own internal approval practices.

Some requests may require supervisor approval.

Others may require departmental coordination.

Carrier Group Administrators should work within these established practices whenever possible.

Application Manager supports the approval process—but organizational governance remains equally important.

7. Managing the User Lifecycle

Ensuring Access Across Employee Relationships

One of the easiest ways to think about Carrier Group Administration is through the lifecycle of an employee.

Application Manager is about more than approving new users.

It's about managing access throughout an employee's relationship with your organization.



New Employee

When a new employee joins your organization:

- confirm their responsibilities,
- ensure they create an Application Manager account,
- review requested carrier access,
- approve appropriate application access,
- direct them to available user guides.

Providing employees with timely access helps them become productive more quickly.



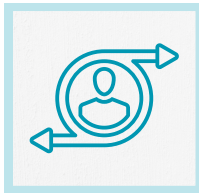
Existing Employee

Employees frequently assume new responsibilities.

When responsibilities change:

- review current permissions,
- determine whether additional applications are needed,
- remove applications that are no longer required.

Application Manager should evolve alongside the employee's responsibilities.



Department Transfer

Employees transferring between departments often require different applications.

Rather than simply adding new access, review existing permissions to determine whether previous access should be modified or removed.

This helps prevent unnecessary accumulation of permissions over time.



Promotion

Leadership roles sometimes require broader application access.

Review requested permissions carefully while ensuring they remain appropriate for the individual's responsibilities.



Employee Departure

When an employee leaves the organization:

- remove Application Manager access promptly,
- verify unnecessary permissions have been removed,
- update organizational records if necessary.

Timely removal of access represents one of the most important security responsibilities performed by Carrier Group Administrators.



Organizational Changes

From time to time, organizations experience:

- restructuring,
- mergers,
- departmental changes,
- staffing adjustments.

These events often require broader review of Application Manager access.

Carrier Group Administrators should use these opportunities to confirm organizational information remains current and user permissions continue reflecting actual business responsibilities.



Looking at the Big Picture

Successful Carrier Group Administrators don't think only about today's access requests.

They think about the entire lifecycle of organizational access—from onboarding new employees to supporting staffing changes and ensuring access remains appropriate throughout an employee's time with the organization.

That long-term perspective helps maintain both security and operational efficiency.



8. Best Practices



What Successful Carrier Group Administration Looks Like

Application Manager provides the tools to manage access. Carrier Group Administrators help ensure those tools are used consistently, securely, and effectively.

The following best practices are not system requirements—they are recommendations that can help your organization maintain efficient operations while reducing administrative effort over time.



Make Access Decisions Promptly

Employees often require Application Manager access to begin performing important job responsibilities. Reviewing requests in a timely manner helps minimize delays while supporting a positive user experience.

Consider establishing an internal expectation for how quickly access requests will be reviewed and, when appropriate, approved.



Apply the Principle of Business Need

Application access should always be based on an employee's current responsibilities.

Rather than approving every requested application, consider whether each application is necessary for the individual's role. Granting only the access employees need helps maintain security while reducing unnecessary complexity.



Keep Access Current

Organizations change continually. Employees join, leave, transfer departments, and assume new responsibilities.

Reviewing user access throughout the year helps ensure Application Manager continues to reflect your organization's current structure.

Small updates performed regularly are typically easier than large-scale cleanup efforts later.

Review Before You Add

When employees request additional applications, take a moment to review their existing permissions.

Sometimes a request reflects changing responsibilities that also warrant removing access to applications the employee no longer needs.

Periodic review helps prevent "permission creep," where users gradually accumulate unnecessary access over time.



Communicate With Department Managers

Carrier Group Administrators are not expected to know every employee's responsibilities.

When questions arise, consult supervisors or department managers before approving unfamiliar requests.

Collaborative decisions typically result in more accurate and appropriate access.



Maintain Multiple Carrier Group Administrators

Whenever practical, designate at least two Carrier Group Administrators.

Having multiple administrators helps ensure:

- User requests continue to be reviewed during vacations or absences.
- Organizational knowledge is retained during staffing changes.
- Access requests are not delayed because only one individual can perform approvals.

Business continuity is one of the simplest—and most valuable—steps an organization can take.



Encourage Self-Service

Many Application Manager questions can be answered through existing resources.

Direct users to:

- Application Manager User Guides
- FAQs
- Quick Start Guides
- Central Support resources

Helping users become more self-sufficient reduces repetitive questions and allows Carrier Group Administrators to focus on access decisions.



9. Common Scenarios

Success Starts With Preparation

Most Carrier Group Administrators encounter the same types of situations throughout the year.

Understanding how to approach these common scenarios can help ensure consistent decision-making.



Scenario: A New Employee Needs Access

A recently hired employee needs access to PCRB/DCRB applications.

Recommended approach:

- Confirm the employee has created an Application Manager account.
- Verify the appropriate user profile.
- Determine which applications are required for the employee's responsibilities.
- Approve access as appropriate.
- Encourage the employee to review available user guides and resources.

Remember that access should support the individual's role—not simply mirror another employee's permissions.



Scenario: An Employee Requests Additional Applications

An employee who already has Application Manager access requests another application.

Before approving the request:

- Determine why the additional application is needed.
- Confirm the request aligns with current responsibilities.
- Review existing permissions to determine whether any applications are no longer required.

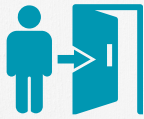


Scenario: An Employee Changes Departments

Department changes often require both adding and removing application access.

Review the employee's complete set of permissions rather than focusing only on the newly requested applications.

The objective is to ensure Application Manager reflects the employee's new responsibilities.

**Scenario: An Employee Leaves the Organization**

Removing access promptly is one of the Carrier Group Administrator's most important security responsibilities.

When an employee leaves:

- Review Application Manager access.
- Remove carrier and application access that is no longer required.
- Confirm organizational records remain current.

Prompt action helps protect both your organization and PCRB/DCRB systems.

**Scenario: A Carrier Group Administrator Leaves**

Business continuity planning should anticipate this possibility.

Whenever practical:

- Maintain multiple Carrier Group Administrators.
- Update organizational contacts promptly.
- Ensure another administrator can continue reviewing requests without interruption.

**Scenario: You're Unsure Whether to Approve a Request**

Occasionally, a request may not clearly align with an employee's responsibilities.

In these situations:

- Request clarification from the employee.
- Consult the employee's supervisor or department manager.
- Contact Central Support if additional guidance is needed.

Thoughtful review is always preferable to making assumptions.

10. Annual Responsibilities

Success Starts With Preparation

Although Carrier Group Administration involves ongoing activities throughout the year, organizations benefit from periodically stepping back and reviewing Application Manager from a broader perspective.

An annual review helps confirm that user access, organizational information, and administrative practices continue to reflect current business needs.



Review User Access

At least once each year:

- Review active users.
- Confirm each individual still requires Application Manager access.
- Verify application permissions remain appropriate.
- Remove unnecessary access.

This review is particularly valuable following organizational restructuring or significant staffing changes.



Review Organizational Information

Confirm that:

- Organizational contacts remain current.
- Carrier Group Administrator information is accurate.
- Internal responsibilities have not changed.

Accurate information helps ensure communications and operational processes continue without interruption.



Evaluate Business Continuity

Ask the following questions:

- Do we have enough Carrier Group Administrators?
- Would access approvals continue if one administrator were unavailable?
- Are our internal procedures documented?

Organizations that plan ahead are better positioned to respond to staffing changes.

Review Security Practices

Annual reviews also provide an opportunity to evaluate broader access management practices.

Consider:

- Are permissions consistently aligned with business responsibilities?
- Have former employees been removed?
- Are there users with unnecessary application access?
- Are approval practices being applied consistently?

Prepare for the Coming Year

Application Manager continues to evolve as PCRB/DCRB introduces new tools, services, and member resources.

Use the annual review to identify opportunities for improving your organization's access management practices and preparing users for upcoming changes.



Open Certification

As part of their ongoing responsibilities, Carrier Group Administrators participate in PCRB/DCRB's annual Open Certification period, which provides an opportunity to review and certify key information associated with their organization in Member Connect, the PCRB/DCRB's secure online platform enabling administrators to view, update, and maintain contact details to ensure regulatory notices and communications reach the right people.

Open Certification helps ensure that organizational information and access remain current and provides a consistent annual checkpoint for CGAs to review information they help maintain throughout the year.

During the Open Certification period, CGAs should:

- Review the information presented for certification.
- Confirm that information is complete and accurate.
- Make or coordinate any necessary updates.
- Complete certification by the established deadline.
- Contact Central Support if questions or discrepancies arise.

PCRB/DCRB will communicate the annual Open Certification period, deadlines, instructions, and available resources directly to CGAs.



Make Certification Easier Throughout the Year

Open Certification should reinforce—not replace—good year-round administration. Keeping user access and organizational information current as changes occur makes the annual certification process faster and easier to complete.

For current dates, instructions, FAQs, and related materials, visit the PCRB/DCRB website's CGA Central page.



Annual Review Calendar

Although each organization should establish practices appropriate to its own operations, the following schedule provides a useful framework.

Quarterly

- Review pending requests.
- Update organizational contacts as needed.
- Remove unnecessary access resulting from staffing changes.

Semiannually

- Review application permissions for key users.
- Evaluate Carrier Group Administrator coverage.

Annually

- Conduct a comprehensive access review.
- Verify organizational information.
- Review business continuity planning.
- Complete the Carrier Group Administrator Annual Checklist included in this playbook.

Regular review helps ensure Application Manager continues supporting your organization's operational needs while maintaining secure and appropriate access.

11. Resources

How to Find What You Need

One of the Carrier Group Administrator's greatest strengths is knowing where to find reliable information.

While this playbook provides guidance on fulfilling the CGA role, many day-to-day tasks are supported by additional PCRB/DCRB resources.

Becoming familiar with these resources will help you answer questions more quickly, make informed decisions, and support users throughout your organization.

Application Manager

Application Manager is the secure gateway to PCRB/DCRB online applications and services. As a Carrier Group Administrator, you will use Application Manager to review requests, manage carrier access, and administer user permissions.

Application Manager User Guide

The User Guide contains detailed instructions for completing tasks within Application Manager.

Use the User Guide when you need step-by-step procedures for:

- Creating and managing user profiles
- Reviewing carrier access
- Approving application requests
- Managing permissions
- Navigating Application Manager

Application User Access Guide

The User Access Guide identifies the applications available to each user type.

Use this resource when determining:

- Which applications may be requested
- Which user types are eligible for access
- Whether an application is available to a particular organization

Bookmark Application Manager & CGA Central Pages

These PCRB/DCRB webpages offer convenient access to the essential guidance, resources, FAQs and tools referenced on these pages and designed to help you manage access and organizational responsibilities.

PCRB Application User Access Guide		Carrier Group Administrator (CGA)	Carrier Group User (CGU)	TPA/ TPE/ MGA	Agent User	Employer User	Guest User	Insurance Department (Admin/User)
Applications		Member carrier admin who manage user access and permissions for their organization.	For employees of member carriers, requiring approval from CGA.	For those that process insurance transactions for a carrier, requiring approval from CGA.	For authorized agents & brokers, requiring approval from Agency Group Administrator (AGA).	For business owners, requiring approval from their Employee Group Administrator (EGA).	For those not associated with any other user type. Does not require admin approval.	For employees of PA Insurance Dept., requiring approval from Insurance Dept. Admin.
WorkComp360		✓	✗	✗	✗	✗	✗	✗
WorkComp360 - Statewide Lens		✓	✓	✓	✓	✓	✓	✓
DataPro+		✓	✗	✗	✗	✗	✗	✗
Carrier Pricing Benchmark		✓	✓	✓	✓	✓	✓	✓
Experience Modification Calculator		✓	✓	✓	✓	✓	✓	✓
Rating & Underwriting Reference		✓	✓	✓	✓	✓	✓	✓
View Authorized Class		✓	✓	✓	✓	✓	✓	✓
Policy Data Manager		✓	✗	✗	✗	✗	✗	✗
Unit Data Manager		✓	✗	✗	✗	✗	✗	✗
Medical Data Call Manager		!	✗	✗	✗	✗	✗	✗
Indemnity Data Manager		!	✗	✗	✗	✗	✗	✗
Test Audit Online		!	✗	✗	✗	✗	✗	✗
Invoice Online		✓	✗	✗	✗	✗	✗	✗
Member Connect		✓	✗	✗	✗	✗	✗	✗
APPLICATION KEY		ACCESS KEY		NEED HELP?				
Data Analytics		Market/Underwriting		Full Access		Requires Department Admin or CGA Approval		
Data Management		Membership		Not Permitted		Requires PCRB Approval		
						Need Help? Email PCRB Central Support at central.support@pcrb.com		

DCRB Application User Access Guide		Carrier Group Administrator (CGA)	Carrier Group User (CGU)	TPA/ TPE/ MGA	Agent User	Employer User	Guest User	Insurance Department (Admin/User)
Applications		Member carrier admin who manage user access and permissions for their organization.	For employees of member carriers, requiring approval from CGA.	For those that process insurance transactions for a carrier, requiring approval from CGA.	For authorized agents & brokers, requiring approval from Agency Group Administrator (AGA).	For business owners, requiring approval from their Employee Group Administrator (EGA).	For those not associated with any other user type. Does not require admin approval.	For employees of DE Insurance Dept., requiring approval from DOI Admin.
WorkComp360		✓	✗	✗	✗	✗	✗	✗
WorkComp360 - Statewide Lens		✓	✓	✓	✓	✓	✓	✓
DataPro+		✓	✗	✗	✗	✗	✗	✗
Carrier Pricing Benchmark		✓	✓	✓	✓	✓	✓	✓
Experience Modification Calculator		✓	✓	✓	✓	✓	✓	✓
Rating & Underwriting Reference		✓	✓	✓	✓	✓	✓	✓
View Authorized Class		✓	✓	✓	✓	✓	✓	✓
Policy Data Manager		✓	✗	✗	✗	✗	✗	✗
Unit Data Manager		✓	✗	✗	✗	✗	✗	✗
Medical Data Call Manager		!	✗	✗	✗	✗	✗	✗
Indemnity Data Manager		!	✗	✗	✗	✗	✗	✗
Delaware Insurance Plan Manager		✗	✗	✗	✗	✗	✗	✗
Invoice Online		✓	✗	✗	✗	✗	✗	✗
Member Connect		✓	✗	✗	✗	✗	✗	✗
APPLICATION KEY		ACCESS KEY		NEED HELP?				
Data Analytics		Market/Underwriting		Full Access		Requires Department Admin or CGA Approval		
Data Management		Membership		Not Permitted		Requires DCRB Approval		
						Need Help? Email DCRB Central Support at central.support@dcrb.com		



Frequently Asked Questions

The FAQ available in this Playbook and on PCRB and DCRB's CGA Central pages answers many common questions related to:

- Accounts
- User Profiles
- Carrier Access
- Application Access
- Registration
- Organizational administration

Central Support

Central Support is available whenever questions cannot be resolved through existing documentation.

Examples include:

- Unusual access requests
- Organizational changes
- Technical issues
- Questions regarding Application Manager administration

Email centralsupport@pcrb.com or centralsupport@dcrb.com or call 215-320-4933.



Building Your Own Internal Resources

Many organizations also develop internal procedures describing:

- Who approves requests
- Department-specific application recommendations
- Employee onboarding procedures
- Offboarding procedures
- Internal approval workflows

These procedures complement Application Manager while reflecting your organization's unique operational practices.

12. Frequently Asked Questions

This chapter addresses questions Carrier Group Administrators commonly encounter.

UNDERSTANDING THE ROLE

What is a Carrier Group Administrator?

A Carrier Group Administrator is the individual designated by a member carrier to manage Application Manager access on behalf of the organization.

The CGA reviews user requests, manages permissions, and helps ensure employees have appropriate access to PCR/DCRB applications.

Why is this role important?

Carrier Group Administrators help maintain secure access, support operational continuity, protect organizational information, and ensure employees can efficiently perform their responsibilities.

Should our organization have more than one CGA?

Whenever practical, yes.

Maintaining multiple Carrier Group Administrators helps ensure access requests continue to be processed during vacations, illnesses, staffing changes, or other absences.

USER MANAGEMENT

How do I know whether someone should receive access?

Consider whether:

- The individual represents your organization.
- The requested application supports their job responsibilities.
- The requested access aligns with your organization's internal practices.

When questions remain, seek clarification before approving the request.

How quickly should requests be reviewed?

Organizations should establish internal expectations that balance thoughtful review with timely service.

Employees often require application access to perform their responsibilities, so unnecessary delays should be avoided.

What if I approve something by mistake?

Review the user's permissions and update access as appropriate.

If additional assistance is required, contact Central Support.

Should I automatically approve requests from managers?

No.

Approval decisions should always be based on business need rather than organizational title. Managers may require broader access—but that determination should still be made thoughtfully.

ORGANIZATIONAL ADMINISTRATION

How often should user access be reviewed?

Periodic review throughout the year is recommended, with a comprehensive review conducted at least annually.

What if our organization reorganizes?

Organizational changes often affect application access.

Following significant restructuring, review:

- User permissions
- Organizational information
- Carrier Group Administrator coverage

What if our Carrier Group Administrator retires or changes roles?

Promptly designate a replacement and update organizational information.

Maintaining multiple Carrier Group Administrators helps minimize disruption.

How can we improve our internal approval process?

Many organizations benefit from:

- Clearly documenting approval responsibilities.
- Coordinating with department managers.
- Periodically reviewing application permissions.
- Establishing expectations for response times.

SUPPORT

Where should users go for help?

Users should first consult:

- Application Manager and CGA webpages/resources
- User Guides
- FAQs

If additional assistance is required, Central Support is available.

When should I contact Central Support?

Examples include:

- Questions regarding unusual access situations.
- Organizational changes affecting Application Manager.
- Technical issues.
- Questions not addressed by existing documentation.

13. Annual CGA Checklist

Application Manager should reflect your organization's current structure.

Completing an annual review helps ensure user access remains appropriate and your organization is prepared to complete Open Certification. Throughout the year, CGAs should continue making updates as changes occur rather than waiting for the annual review.

User Access Review

- ☐ Review all active users.
- ☐ Confirm each individual still requires Application Manager access.
- ☐ Verify application permissions remain appropriate.
- ☐ Remove unnecessary access.
- ☐ Confirm new employees have appropriate access.

Organizational Information

- ☐ Review organizational contacts.
- ☐ Confirm Carrier Group Administrator information is current.
- ☐ Update organizational information when necessary.
- ☐ Verify departmental responsibilities have not significantly changed.

Open Certification

- ☐ Review current Open Certification instructions and deadlines
- ☐ Complete required review and updates
- ☐ Submit certification by the deadline.
- ☐ Contact Central Support if you identify discrepancies or need assistance.

Security

- ☐ Remove former employees.
- ☐ Review users with elevated permissions.
- ☐ Confirm permissions continue supporting legitimate business needs.
- ☐ Address inactive or unnecessary accounts.

Business Continuity

- ☐ Confirm at least two Carrier Group Administrators are available whenever practical.
- ☐ Review internal approval procedures.
- ☐ Ensure another administrator can continue approvals if needed.
- ☐ Update internal documentation as appropriate.

Communications

- ☐ Review recent PCRB/DCRB communications.
- ☐ Share important updates with affected departments.
- ☐ Identify new resources that should be communicated internally.

Looking Ahead

- ☐ Determine whether additional employees may require access to new PCRB/DCRB applications.
- ☐ Identify opportunities to improve internal approval processes.
- ☐ Schedule next year's access review.

Final Thoughts

Carrier Group Administration is an ongoing organizational responsibility—not simply an administrative task completed when employees are hired.

By periodically reviewing access, maintaining accurate information, and thoughtfully evaluating user requests, Carrier Group Administrators help create a secure, efficient, and reliable environment that benefits both their organizations and the broader PCRB/DCRB membership community.

Thank you for serving in this important role.



Carrier Group Administrators play a vital role in connecting your organization to the tools, resources and information it needs

For CGA assistance, please contact:

PCRB/DCRB Central Support

Phone: 215-320-4933

Email: centralsupport@pcrb.com or
centralsupport@dcrb.com