Independent Dispute Resolution (IDR) Gateway

Dispute Processing User Guide

Version 1.0
Release 2
September 2026

Table of Contents

1. Introduction 4

2. IDR Gateway Overview 5
   2.1. The IDR Gateway 5
   2.2. Development Phases 5
   2.3. Who Should Sign Up 5
   2.4. IDR Gateway Access Types 6

3. Identity Verification 7
   3.1. Identity Verification Process 7

4. Create an IDR Gateway Account 8
   4.1. Create an Account with a Credential Service Provider 8
   4.2. Sign In with Existing CMS-Approved Credentials 9
   4.3. First Time Sign In 11

5. Sign In to the IDR Gateway 15

6. Join an Organization 17
   6.1. Accept an Invitation to Join an IDR Gateway Organization 17
   6.2. Search for an Organization to Join 19
   6.3. Leave an Organization 20

7. Review Roles and Workspaces 21
   7.1. Roles 21
   7.2. Workspaces 21
   7.3. View Your Role and Workspace Assignments 23

8. Manage Notifications 24
   8.1. System Notifications 24
   8.2. View Notifications from the Home Page 24
   8.3. Filter and Search for Notifications 25

Appendix A. Resources 27
   IDR Gateway Help Desk Resources 27
   IDR Resources 27

Appendix B. Warning and Security & Privacy Agreement 28

Appendix C. IDR Gateway Rules of Behavior 31

Appendix D. Acronyms & Terms 33

Table of Figures

Figure 1. IDR Gateway Access Page 8
Figure 2. Sign In/Create Your CMS Account Page 9
Figure 3. Verify Your Identity Message 10
Figure 4. Warning and Security & Privacy Agreement Window 11
Figure 5. Rules of Behavior Window 12
Figure 6. Set Up Your Profile Window (Select Affiliation and Confirm Email) 13
Figure 7. Set Up Your Profile Window (Confirmation) 14
Figure 8. Sign In/Create Your CMS Account Page 15
Figure 9. Rules of Behavior Window 16
Figure 10. Invitation to Join an Organization Notification 17
Figure 11. My Profile Page (Invitations Section) 17
Figure 12. Accept Invitation Confirmation 18
Figure 13. My Organization (Invitation Accepted) 18
Figure 14. Search for Your Organization Field 19
Figure 15. My Organization (Search Result Found) 20
Figure 16. Workspace Example 22
Figure 17. My Organization Section 23

Figure 18. IDR Gateway Home Menu Bar 24
Figure 19. My Notifications Table 24
Figure 20. View All Notifications Button 25
Figure 21. My Notifications Page (All Active Tab)..... 26

1. Introduction

Welcome to the IDR Gateway Dispute Processing User Guide

This user guide supports Independent Dispute Resolution (IDR) Gateway verified users. It provides information and step-by-step instructions to create an account, join an organization, and manage notifications within the IDR Gateway.

More features are coming soon.

The IDR Gateway is a sign-in community that provides a secure, centralized platform to manage payment disputes. It allows users to securely access all related disputes, submit necessary forms, and easily track progress through reports and dashboards.

What You'll Learn

This user guide provides information about how to:

- **Create an IDR Gateway Account.** Get started by setting up your account.
- **Sign In to the IDR Gateway.** Access the system with your credentials.
- **Join an Organization.** Gain access to the dispute dashboards and reports for your organization within the IDR Gateway.
- **Review Role and Workspaces.** Learn how administrators can use roles and workspaces to limit user access and user actions on disputes.
- **Manage Notifications.** Manage notification settings to stay informed about updates or actions related to your organization.

Updated user guides are published on the CMS.gov IDR Gateway page with every IDR Gateway phase. Check back for information about new IDR Gateway features.

Let's get started!

If you are an administrator, you can access the **IDR Gateway Administrator Guide** on the IDR Gateway page.

2. IDR Gateway Overview

2.1. The IDR Gateway

The IDR Gateway is a sign-in community that transitions the Federal IDR process from single-use web forms to a secure, centralized platform that parties can use to manage disputes. IDR Gateway users will be able to:

- Start and respond to disputes.
- Access dispute dashboards and reports associated with their organization.
- Track dispute information, including disputes assigned to a certified IDR entity.
- Monitor assigned disputes by process phase.
- Review notifications regarding dispute activity.

The IDR Gateway includes important new security features, including identity verification processes and protocols that permit only U.S.-based users to access the Federal IDR process.

2.2. Development Phases

The IDR Gateway will roll out in phases. In Phase 1, administrators can sign up and set up their organizations in the IDR Gateway. In Phase 2, users who are responsible for submitting dispute web forms can sign up and join an organization. During these first two phases (the sign-up period), disputes in the Federal IDR process will continue to operate through the current web forms and not in the IDR Gateway.

Once the sign-up period is complete, the Federal IDR process will fully transition into the IDR Gateway (Phase 3), integrating existing web forms and introducing new dispute dashboards and reports. Parties will need an IDR Gateway account to submit web forms through the new IDR Gateway to continue participating in the Federal IDR process. Only users who have joined an organization can access the dispute dashboards and reports linked to their organization to track the status of their disputes.

IDR Gateway access is only available for individuals located in the U.S. and its territories. This system blocks users who try to access the IDR Gateway from outside the U.S. or its territories.

2.3. Who Should Sign Up

Organizations that handle dispute processing must create IDR Gateway accounts. If you or your staff currently submit IDR web forms in the current Federal IDR process, you must sign up to use the IDR Gateway. If your organization is named in disputes but relies on a third-party administrator (TPA) or other organization to manage dispute processing activities, your organization does not need to sign up for the IDR Gateway itself, but must ensure the TPA or organization responsible for managing dispute processing activities creates an IDR Gateway account.

Within the IDR Gateway, an organization is considered any company or enterprise that manages dispute processing.

Important: The IDR Gateway does not have any features that link one organization to another. Therefore, organizations named in disputes but not involved in the day-to-day management of disputes should not create an IDR Gateway account. For example, if Dr. Smith uses Corporation A to manage Federal IDR disputes, Corporation A should set up an account, but Dr. Smith should

not. If an organization named in disputes uses a third-party dispute processing company and wants to track its IDR disputes, it should ask its dispute processing company for a report. Administrators are able to export reports of dispute activity they can provide to parties named in disputes that do not have IDR Gateway accounts. If an entity manages some of its disputes itself but also uses one or more third-party dispute processing companies to manage its other disputes, the entity should set up an IDR Gateway account for the disputes they manage.

2.4. IDR Gateway Access Types

There are two types of access to the IDR Gateway: administrator and verified. After creating an account, your access type displays on the “My Profile” page.

Verified Access

Users who successfully complete identity verification have verified access, which allows the user to start and respond to disputes, along with the ability to join an organization and access associated dashboards and reports.

Administrator Access

Administrators have the same abilities as verified users to start and respond to disputes and view dashboards and reports. Administrators are also responsible for creating organizations in the IDR Gateway, managing organization information, inviting users to join their organization, and managing user access.

Organizations must have at least one administrator but may have between 2–10 administrators depending on the size of the organization. It is recommended that organizations should have a sufficient number of administrators to ensure timely handling of user access requests and organization updates.

3. Identity Verification

All IDR Gateway users must verify their identity with an approved credential service provider during the account creation process. Individuals who do not verify their identity cannot access the IDR Gateway. This requirement helps to prevent fraud and unauthorized access.

A **credential service provider** is a trusted entity whose functions include identity proofing applicants and registering authenticators to subscriber accounts. A credential service provider may be an independent third party.

If new users have previously verified their identity through an approved credential service provider (e.g., Identity Management [IDM] service or Login.gov), they can log in to the IDR Gateway using those credentials. If they have not previously verified their identity, they must create a new account with an approved credential service provider and complete the identity verification process before they can sign in to the IDR Gateway.

3.1. Identity Verification Process

IDR Gateway users who do not already have an account with an approved credential service provider are required to create one. To create an account, you must:

- Sign up using your email address and create a secure password. You may also be asked to set up multi-factor authentication (MFA) for added security.
- Provide identifying information, such as your full name and Social Security Number (SSN) to confirm your identity.
- Verify your identity by submitting a photo ID. You can do this by uploading a photo of an approved ID type and submitting a “selfie” through the credential service provider’s website or application or bringing your approved ID to a location where it can be verified in person.

A credential service provider will use this information to verify your identity. Credential service providers may take different approaches to verifying identity. For details on how your information is used, refer to the credential service provider’s website.

If your identity is successfully verified, you will be able to access the IDR Gateway. If the verification fails, the credential service provider will suggest troubleshooting steps, and alternative verification options.

Credential service providers are responsible for protecting your information and keeping it secure. For more information refer to the credential service provider.

4. Create an IDR Gateway Account

All IDR Gateway users must create an account and complete the identity verification process with an approved credential service provider to log in to the IDR Gateway. A credential service provider is a trusted entity whose functions include identity proofing applicants and registering authenticators for accounts.

- **New Credentials**. New IDR Gateway users without existing credentials must create an IDR Gateway account using an approved credential service provider (Refer to Section 3.1 Identity Verification Process).
- **Existing Credentials**. New IDR Gateway users with existing CMS-approved credentials (such as IDM) or an existing account with another credential service provider on the IDM Sign In page (such as Login.gov) can sign in to the IDR Gateway using those credentials.

4.1. Create an Account with a Credential Service Provider

If you do not have an existing IDR Gateway account or an account with a CMS-approved credential service provider (such as ID.me or Login.gov), complete steps 1-4 to create your account.

1. Navigate to the IDR Gateway Access page.

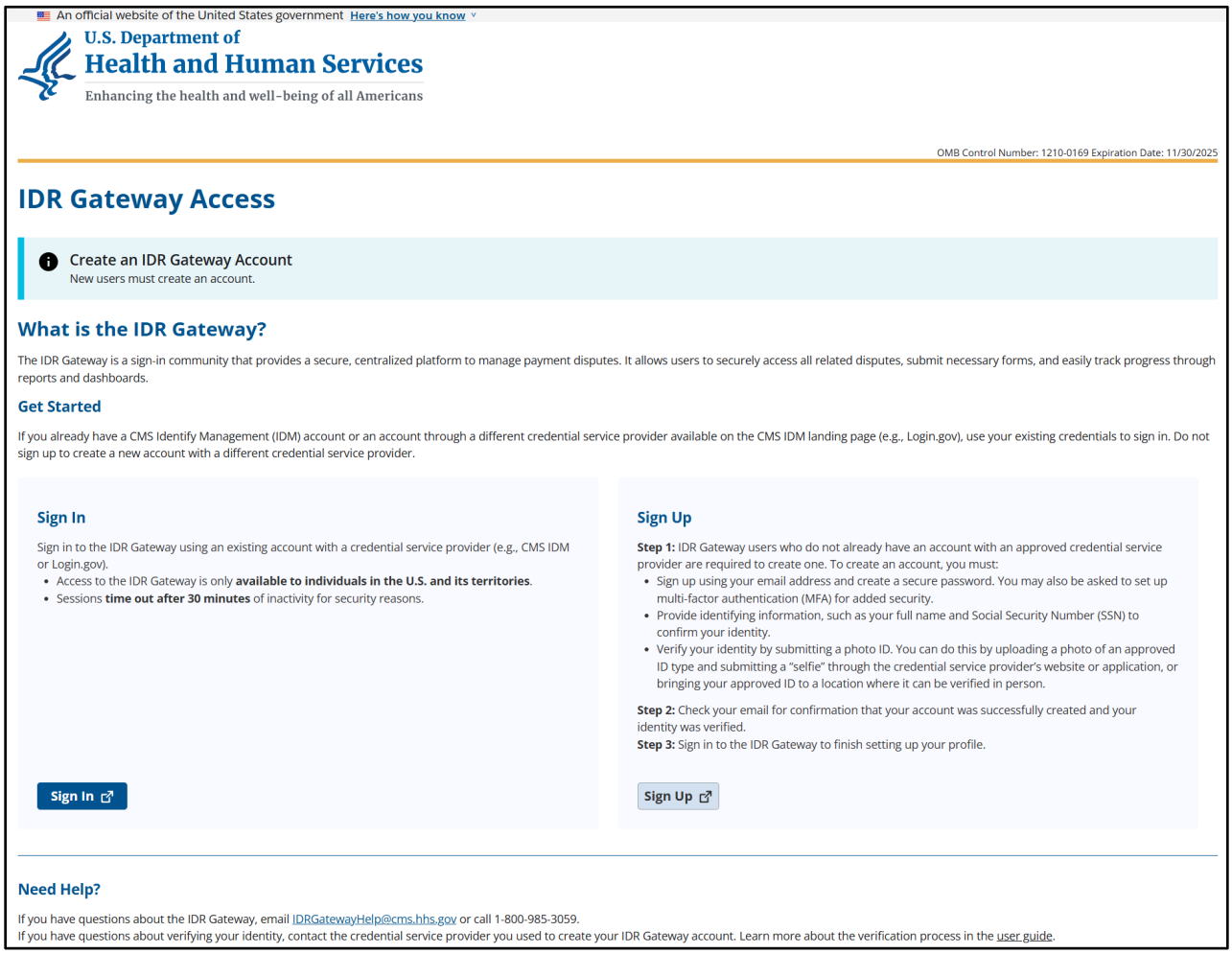

Figure 1. IDR Gateway Access Page

2. From the “IDR Gateway Access” page, select the **Sign Up** button. The “Sign in/Create your CMS account” page displays.

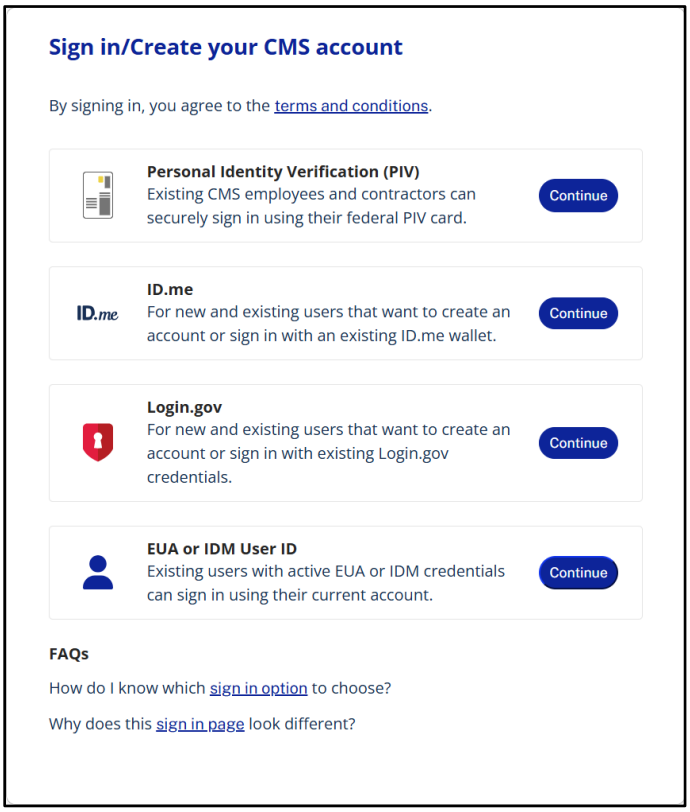

Figure 2. Sign In/Create Your CMS Account Page

3. Select the **Continue** button of your preferred credential service provider from the available choices to start the account creation and identity verification process. During this process, you must create an account and verify your identity before you can access the IDR Gateway. Refer to Section 3. Identity Verification for more information about the identity verification process.
   a. Do not create a new IDM account.
   b. Do not use the PIV option.
4. Upon account creation, continue to Section 4.3. First Time Sign In.

4.2. Sign In with Existing CMS-Approved Credentials

If you have an existing account with a CMS-approved credential service provider, such as ID.me or Login.gov, complete the following steps to sign in to the IDR Gateway.

1. Navigate to the IDR Gateway Access page.
2. From the “IDR Gateway Access” page, select **Sign In**. The “Login/Create your CMS account” page displays.
3. Select the **Continue** button for your preferred credential service provider option.
4. Enter your credentials and select **Submit** to sign in to the IDR Gateway.
   a. If you have an existing CMS-approved account that did not require identity verification the “Verify Your Identity” message displays when signing in to the IDR Gateway for the first time.

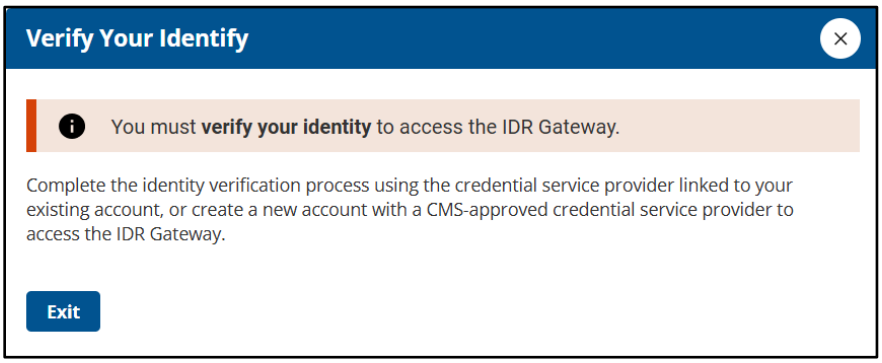

Figure 3. Verify Your Identity Message

b. Select the **Exit** button to close the window.

c. Return to the IDR Gateway Access page and select the **Sign Up** button.

d. Create an account with a credential service provider and complete the identity verification process. Refer to Section 4.1 Create an Account with a Credential Service Provider.

5. Continue to Section 4.3. First Time Sign In.

4.3. First Time Sign In

1. When signing in to the IDR Gateway for the first time, the Warning and Security & Privacy Agreement window opens.

Figure 4. Warning and Security & Privacy Agreement Window

2. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the entire agreement.)

3. Select **Continue**. The Rules of Behavior window opens.

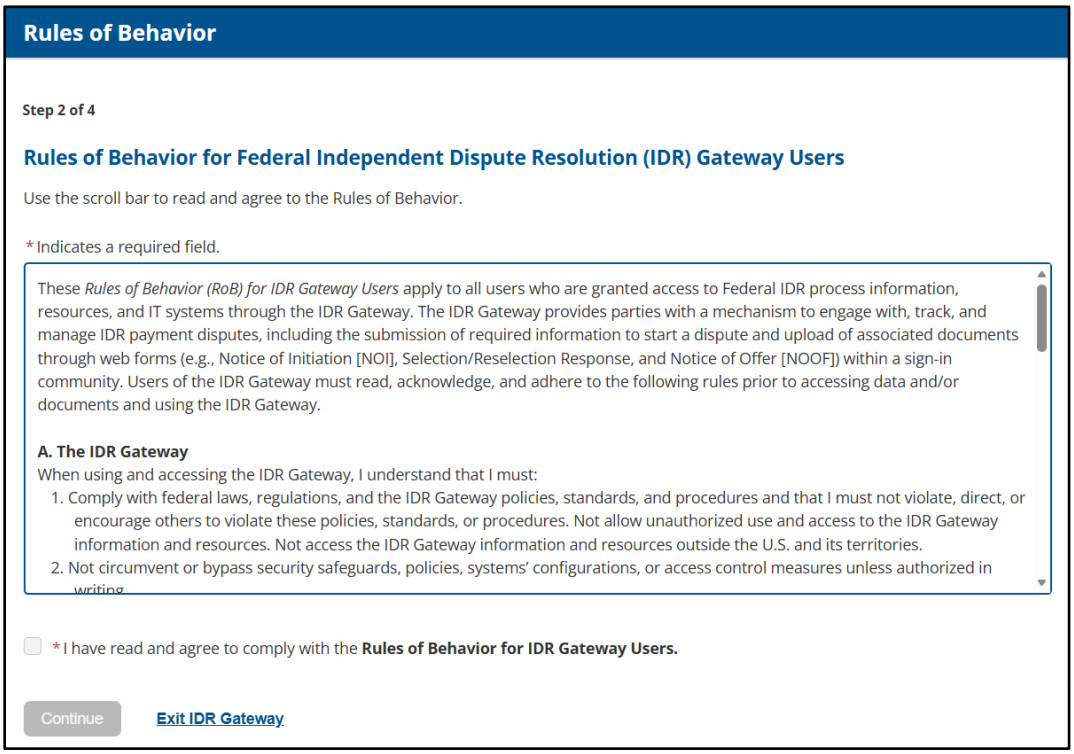

Figure 5. Rules of Behavior Window

4. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the rules.)
5. Select **Continue**. The Set Up Your Profile window opens.

Set Up Your Profile

Step 3 of 4

Select Affiliation and Confirm Email

Choose your affiliation to complete your Independent Dispute Resolution (IDR) Gateway profile.

* Indicates a required field

* **I am here to engage in the Federal IDR process on behalf of a:**

- (●) Provider, Health Care Facility, or Air Ambulance Provider
- ( ) Group Health Plan, Individual Health Insurance Issuer, or Federal Employees Health Benefits (FEHB) carrier

* **The email associated with your sign in credentials is idr.verified.user@gmail.com. Is this the work email you want to use for IDR Gateway notifications?**

- ( ) Yes. This is the email I want to use for IDR Gateway notifications
- (●) No. I want to use a different email for IDR Gateway notifications

Enter the email address you want to use for IDR Gateway notifications.

* **IDR Gateway Notification Email:**

john.smith@test.org

Continue

Figure 6. Set Up Your Profile Window (Select Affiliation and Confirm Email)

6. Select your affiliation from the following options to indicate how you engage with the Federal IDR process:
   a. Provider, Health Care Facility, or Air Ambulance Provider
   b. Group Health Plan, Individual Health Insurance Issuer, or Federal Employees Health Benefits (FEHB) carrier

You only need to indicate your affiliation the first time you sign in to the IDR Gateway.

7. Confirm the displayed email address you used to login is the work email address you would like to use for IDR Gateway notifications.
   a. If you select “No,” a field displays to provide an additional email address to receive IDR Gateway notifications. **Do not use a shared inbox as your IDR Gateway notification email address.**
   b. If you entered an email address for IDR Gateway notifications, you must verify the email address before you can join an organization. Select the verification link in the email message from auto-reply-FederalIDRQuestions@cms.hhs.gov and sign in to the IDR Gateway.

If you enter a shared inbox as your IDR Gateway Notification email address, only you can verify that email address. Anyone else who attempts to verify that email address will receive a “Not Authorized” error message.

8. Select **Continue**.
   a. The Profile setup confirmation displays.

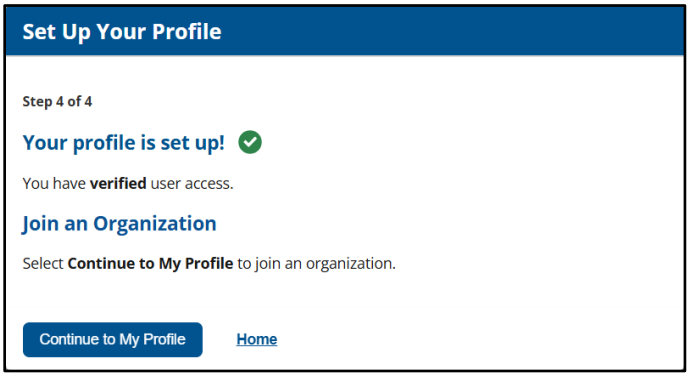

Figure 7. Set Up Your Profile Window (Confirmation)

9. Select the **Continue to My Profile** button.
   a. If you have an existing CMS-approved account but your credential service provider did not verify your identity, a Verify Your Identity alert displays.
   b. Refer to Section 4.1 Create an Account with a Credential Service Provider to complete the identity verification process for your credential service provider.

5. Sign In to the IDR Gateway

After creating an IDR Gateway account, and signing into the IDR Gateway for the first time, you can sign in to the IDR Gateway from the “IDR Gateway Access” page.

1. Navigate to the IDR Gateway Access page.
2. Select the **Sign in** button. The “Sign in/Create your CMS account” page displays.

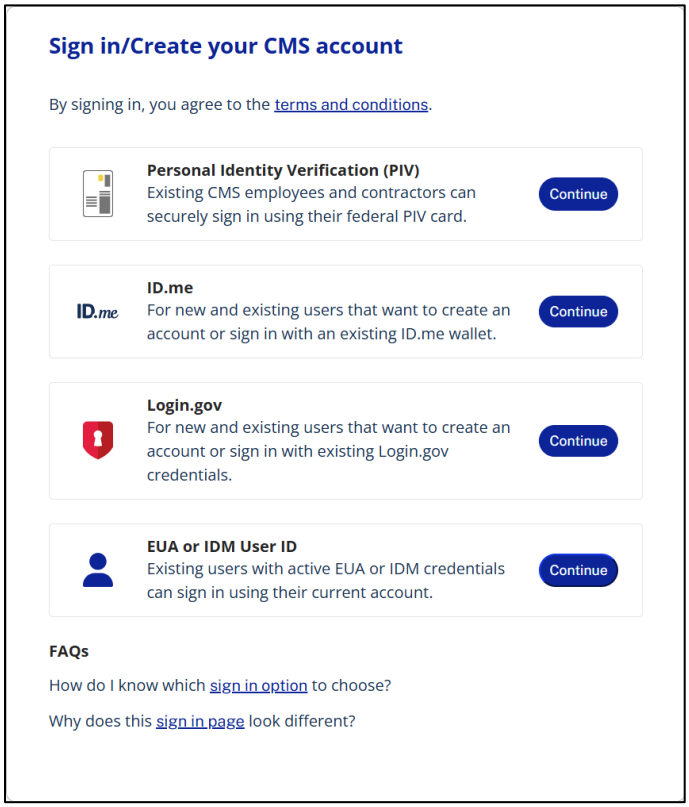

Figure 8. Sign In/Create Your CMS Account Page

3. Select the **Continue** button for the credential service provider you used to create an IDR Gateway account. By signing in, you agree to the terms and conditions.

4. Enter your credentials and select the **Submit** or **Sign in** button (depending on the credential service provider) to sign in to the IDR Gateway. The Rules of Behavior window opens.

Figure 9. Rules of Behavior Window

5. Scroll down, read the agreement, and select the checkbox to agree to the terms. (The checkbox does not activate until you have reviewed the rules.) The "IDR Gateway Home" page displays. Every time you sign in to the IDR Gateway, you must review and agree to the rules of behavior.

6. Join an Organization

An administrator can invite people to join their organization in the IDR Gateway. Joining an organization provides you with access to the organization's dispute dashboards and reports. Receiving an invitation to join an organization is the most common way to join an organization in the IDR Gateway.

If you did not receive an invitation but believe you should be able access the IDR Gateway as part of an organization, refer to Section 6.2 Search for an Organization to Join to search for and request to join an organization.

You can only join one organization at a time.
You must leave an organization before joining a different organization.

6.1. Accept an Invitation to Join an IDR Gateway Organization

If an administrator invites you to join their organization in the IDR Gateway, you will receive an email invitation that expires in 10 business days. If you already have an IDR Gateway account, you will also receive an in-system notification.

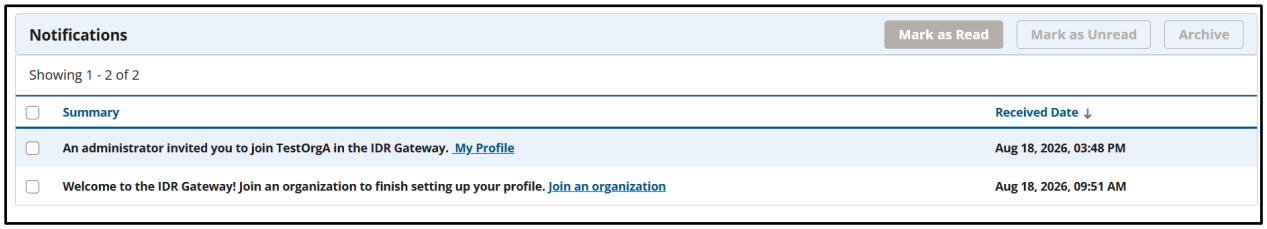

Figure 10. Invitation to Join an Organization Notification

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The "My Profile" page displays.
2. Review the organization information in the "Invitations" section to confirm you belong to this organization.

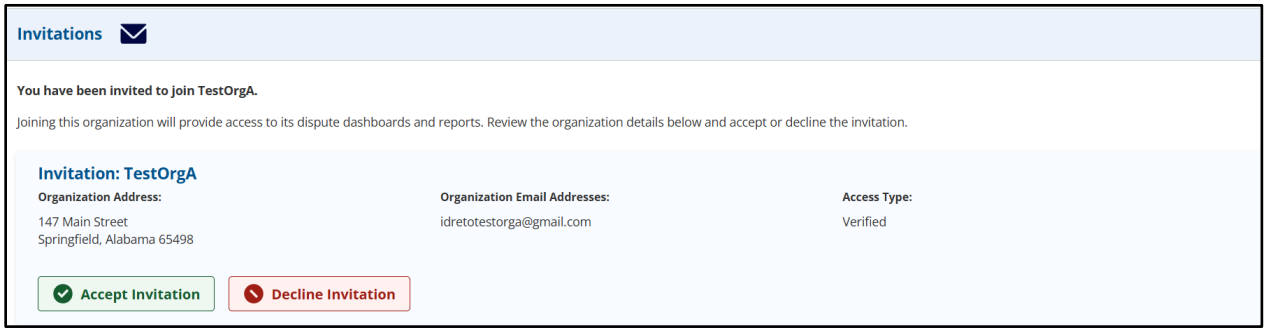

Figure 11. My Profile Page (Invitations Section)

3. Select the **Accept Invitation** or the **Decline Invitation** button. A confirmation message displays.
   a. Accepting the invitation automatically declines other pending invitations.
   b. Accepting the invitation will allow you to access the dispute dashboard or reports for the organization when they become available.

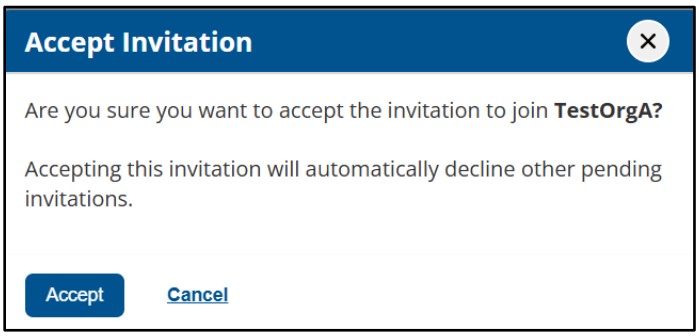

Figure 12. Accept Invitation Confirmation

4. Select the **Accept** button to join the organization. The organization displays in the "My Organization" section of the "My Profile" page.

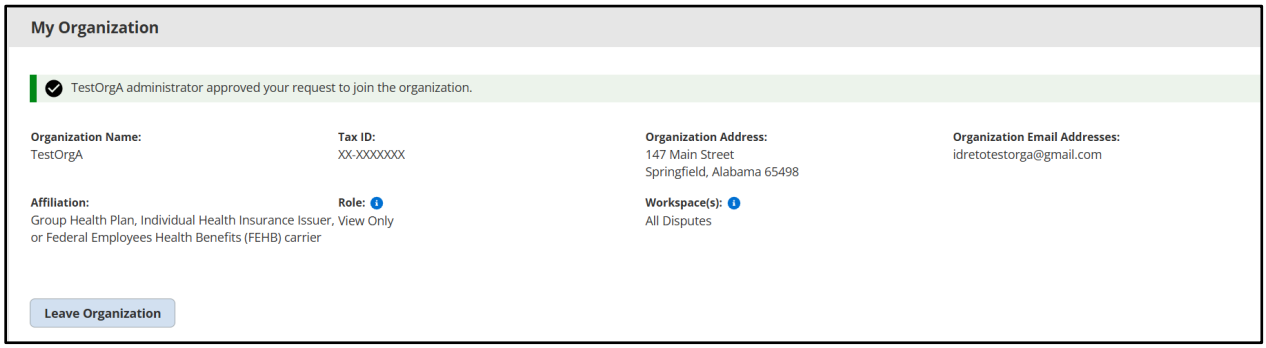

Figure 13. My Organization (Invitation Accepted)

6.2. Search for an Organization to Join

If you did not receive an invitation to join an organization but believe you should be part of an organization in the IDR Gateway, follow these steps to find and join your organization.

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The “My Profile” page displays.
2. From the “My Organization” section, enter the email address associated with the organization in the **Search for Your Organization** field.

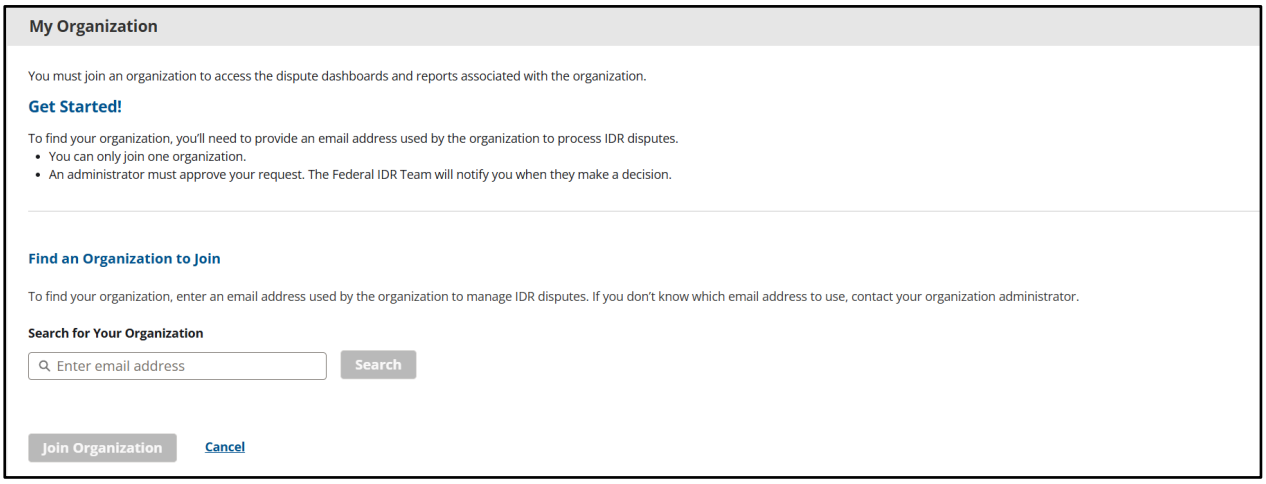

Figure 14. Search for Your Organization Field

3. Select **Search**. The organization linked to the email address displays.
4. If your organization is found, select the **Join Organization** button.
   a. If your organization is not found, verify you entered the correct email address. If the email address is correct, the organization does not exist yet in the IDR Gateway.
   b. If the “Organization setup in progress” alert displays, another user has requested the creation of an organization with the information you provided. Wait until the organization setup is complete, which could take up to two days, and then request to join the organization.
   c. If you believe there is an error, contact IDRGatewayHelp@cms.hhs.gov.

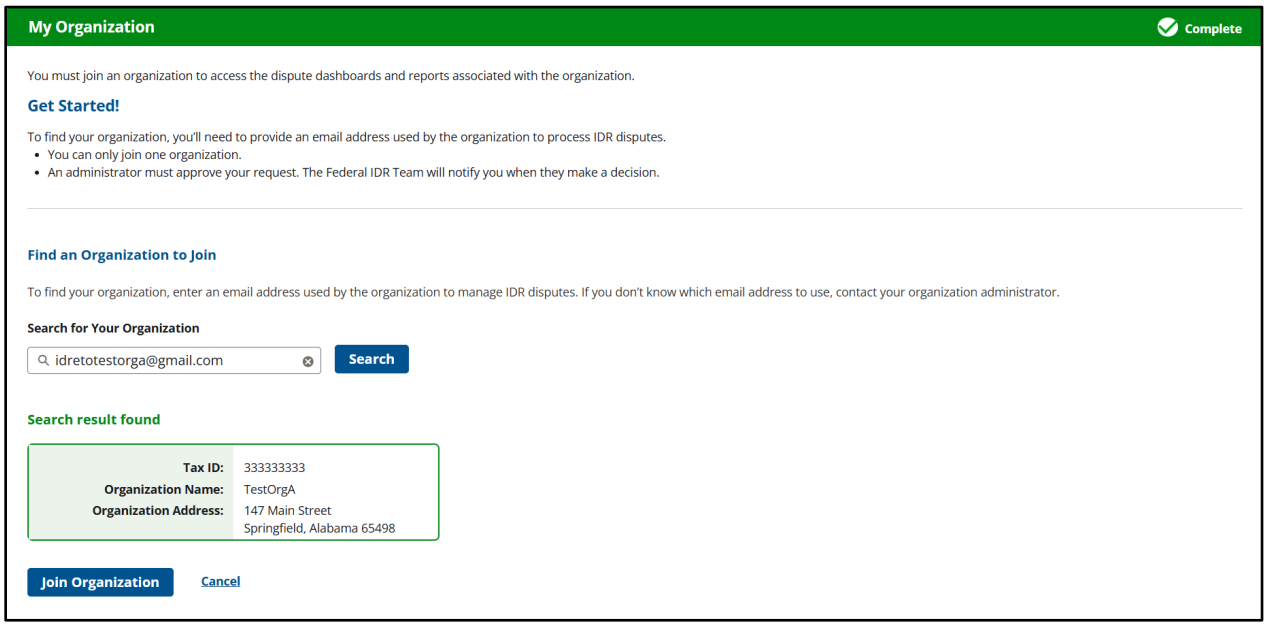

Figure 15. My Organization (Search Result Found)

5. An administrator must review your request to join the organization.
   a. You will be notified when a decision is made.
   b. Once your request to join an organization is approved, you can access organization details from the "Organization Information" page.

6.3. Leave an Organization

Verified users can only join one organization at a time. If you joined an organization in error or want to join a different organization, you can leave your current organization from the "My Profile" page.

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The "My Profile" page displays.
2. In the "My Organization" section, select the **Leave Organization** button.
3. Review and revise your affiliation, if needed.
4. Select the **Confirm** button.

7. Review Roles and Workspaces

When adding a new user to an organization, administrators can use roles and workspaces to limit the disputes a user can access and the actions a user can take on disputes.

7.1. Roles

When an administrator reviews a user request to join their organization, they must assign the new user a role:

- **View Only** roles may view all dispute information but cannot submit web forms.
- **Initiation and Selection** roles can submit initiation, certified IDR entity selection, and reselection web forms, but cannot submit offers or view dispute outcomes.
- **Full Access** roles can view all dispute information and submit all web forms.

7.2. Workspaces

Workspaces are secure spaces that contain a subset of your organization's disputes based on the email addresses listed on the dispute. Workspaces allow administrators to control the disputes a user can access. If you are not assigned to a workspace, you will have access to the All Disputes workspace, which displays all the disputes associated with an organization.

Review the workspaces listed in your "My Organization" section if you think there are disputes that should display but do not.
Contact the organization's administrator with any questions.

Workspace Example

An example where workspaces may be helpful is a large organization with multiple teams that manage disputes through separate inboxes, supporting different clients. In Figure 16, Organization A has three Clients: B, C, and D. Organization A has four users – the administrator,

Alex, Susan, and Jane. The administrator creates three workspaces, one for each client, using the respective dispute processing email addresses.

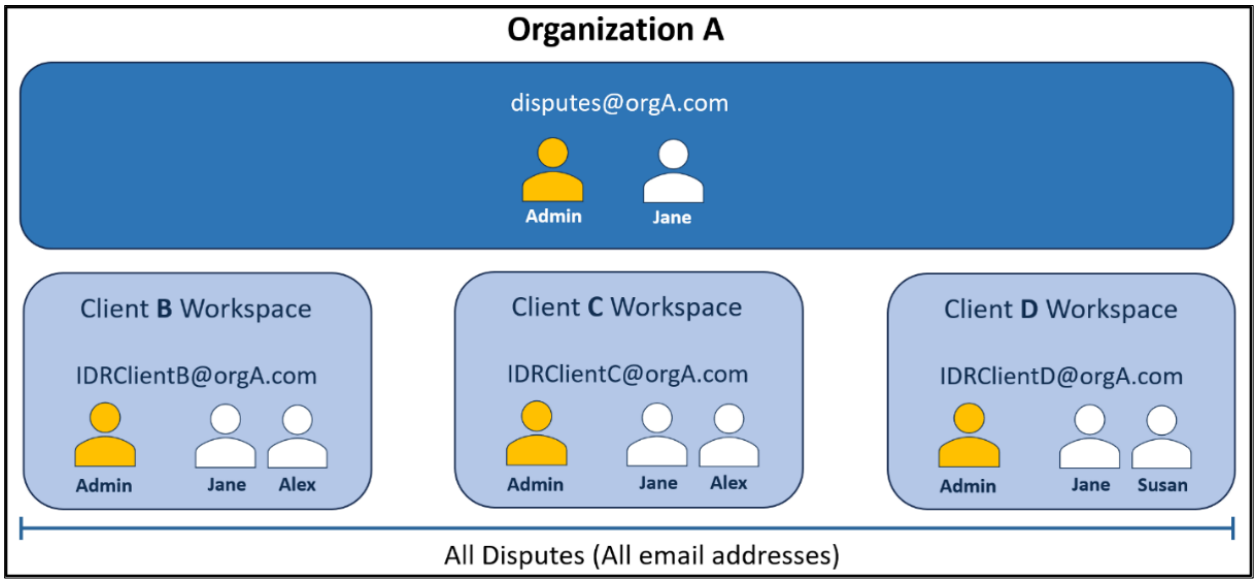

Figure 16. Workspace Example

- Client B's workspace is named Workspace B and uses the inbox email address IDRClientB@email.org.
- Client C's workspace is named Workspace C and uses the inbox email address IDRClientC@email.org.
- Client D's workspace is named Workspace D and uses the inbox email address IDRClientD@email.org.

Alex works on disputes for Client B and Client C, so the administrator assigns Alex to Workspace B and Workspace C. Susan only works on disputes for Client D, so the administrator assigns Susan to Workspace D. Jane works on disputes for all three clients, so the administrator does not assign Jane to any of the workspaces as Jane has access to all disputes through the All Disputes workspace.

7.3. View Your Role and Workspace Assignments

Verified users can view their current role and workspace assignments from the “My Profile” page.

1. From the Home menu bar, select the **My Profile** option from the user menu dropdown list. The “My Profile” page displays.
2. Navigate to the “My Organization” section. The organization displays in the “My Organization” section of the “My Profile” page.

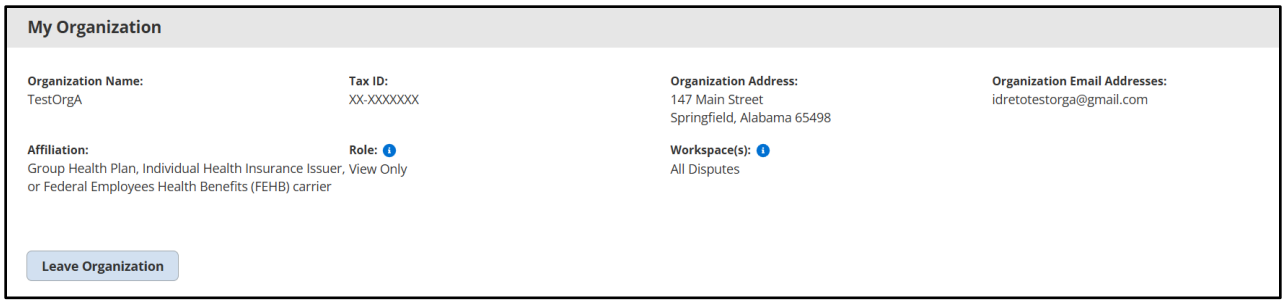

Figure 17. My Organization Section

3. Review the **Role** and **Workspace(s)** fields to find your current assignments.

Contact your administrator if you believe you were assigned the wrong role or workspace. Only an administrator can update user roles and workspace assignments.

8. Manage Notifications

The Home menu bar at the top of every page provides easy navigation to the IDR Gateway "Home" page, the "Notification" page, the user guide, and a dropdown list under the user's name with links to pages specific to the user.

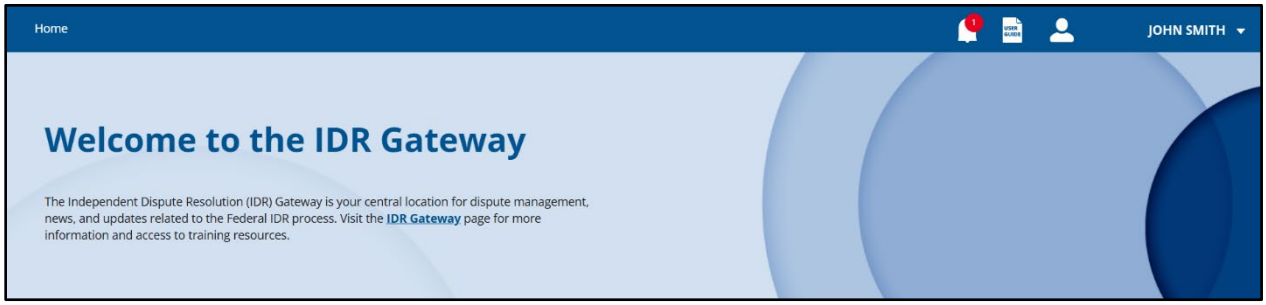

Figure 18. IDR Gateway Home Menu Bar

8.1. System Notifications

System notifications provide important updates or actions related to your account or disputes. Users can view a summary of recent system notifications from the "Home" page or detailed notification information on the "My Notifications" page.

8.2. View Notifications from the Home Page

1. From the Home menu bar, select the **Home** button. The "IDR Gateway Home" page displays.
2. Scroll down to view the My Notifications table.
   a. Notifications are organized by the date they are received.
   b. If a system notification has a supporting email message, the notification summary matches the email subject line. The supporting email message provides additional information not listed in the in-system notifications.
   c. Notifications are marked as read when the user views the notification. Dispute and organization notifications, which display for multiple users, are marked as read when the first user views the notification.
   d. Users can manually mark the notification as unread again for other users associated with the organization.

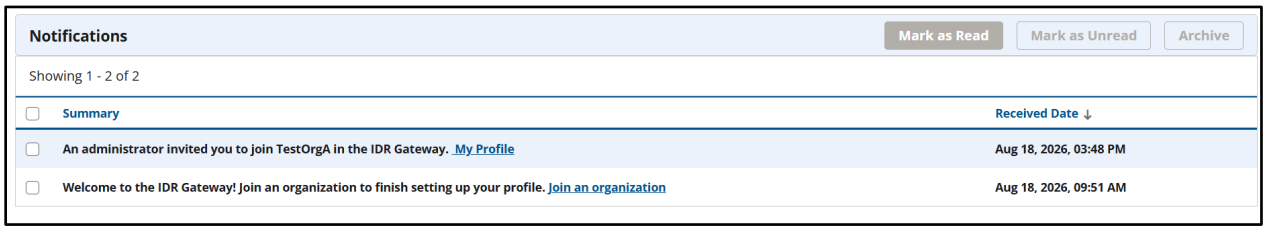

Figure 19. My Notifications Table

Notifications older than 30 business days are automatically archived.

3. Select the checkbox next to a notification to enable the **Mark as Read**, **Mark as Unread**, and **Archive** buttons.
   a. Select **Mark as Read** to unbold the notification title in the Summary column. Notifications will also be marked as read once opened.
   b. Select **Mark as Unread** to bold the notification title in the Summary column.
   c. Select **Archive** to remove the notification title from the Summary column.

8.3. Filter and Search for Notifications

1. From the Home menu bar, select the **Notifications (bell icon)**. The **View All Notifications** button displays.

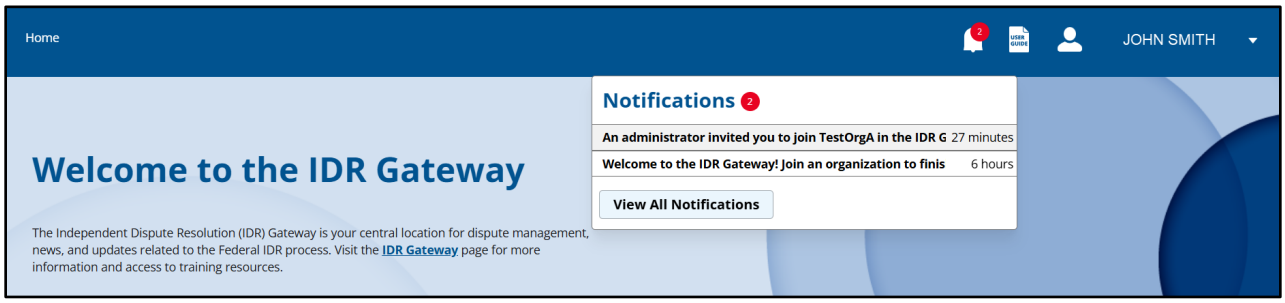

Figure 20. View All Notifications Button

2. Select the **View All Notifications** button. The “My Notifications” page displays.

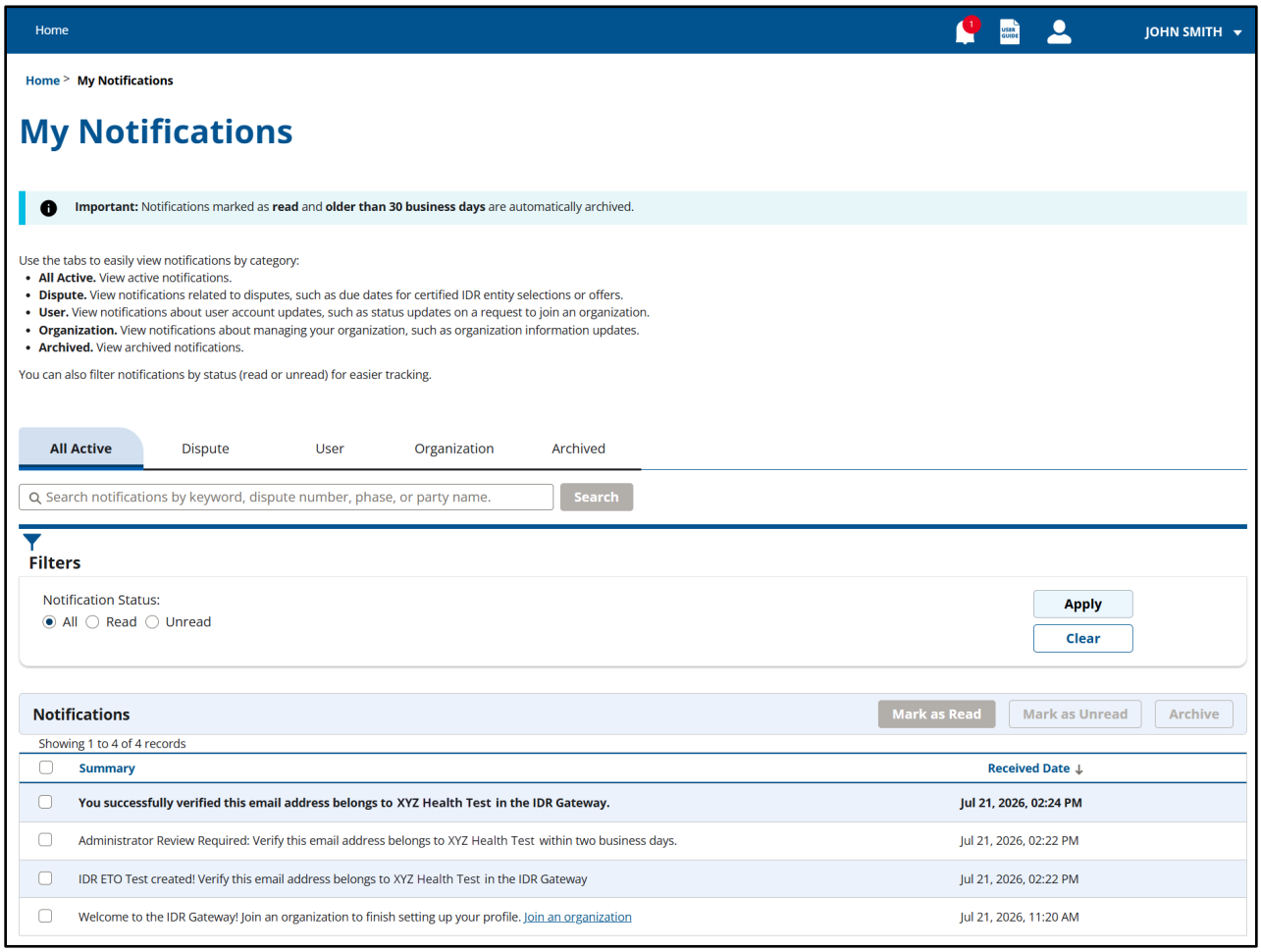

Figure 21. My Notifications Page (All Active Tab)

3. Select a tab to filter the notifications by type.
   a. All Active. View all active notification types (Dispute, User, and Organization). Active notifications include both read and unread notifications that have not been archived.
   b. Dispute. View notifications related to disputes, such as due dates for selecting a certified IDR entity to manage the dispute or to submit offers.
   c. User. View notifications about an individual user’s account updates, such as status updates on a request to join an organization.
   d. Archived. View archived notifications. Archived notifications are older than 30 business days or have been archived by a user using the Archive button.
4. Select a **Notification Status** option (All, Read, Unread) to filter notifications by status.
5. Enter at least three characters of a keyword, dispute number, or party name to search for a notification.
6. Select the **Apply** button to display the resulting notifications.

Appendix A. Resources

This section of the user guide provides helpful resources to help you navigate issues you may encounter while creating an IDR Gateway account and setting up your organization, as well as additional context on the Federal IDR process.

IDR Gateway Help Desk Resources

- **IDR Gateway questions or issues?** Email IDRGatewayHelp@cms.hhs.gov or call 1-800-985-3059.
- **Privacy concerns?** Email Privacy@cms.hhs.gov.
- **Questions or issues related to specific disputes or to the IDR process generally?** Email FederalIDRQuestions@cms.hhs.gov.

IDR Resources

The following resources about the No Surprises Act and the Independent Dispute Resolution are available to IDR Gateway users.

- CMS IDR Gateway page: https://www.cms.gov/nosurprises/help-resolve-payment-disputes/idrgateway
- CMS No Surprises home page: https://www.cms.gov/nosurprises
- CMS No Surprises privacy information: https://www.cms.gov/nosurprises/privacy
- CMS About Independent Dispute Resolution: https://www.cms.gov/nosurprises/help-resolve-payment-disputes/payment-disputes-between-providers-and-health-plans
- Overview of Rules and Fact Sheets related to the No Surprises Act: https://www.cms.gov/nosurprises/policies-and-resources/overview-of-rules-fact-sheets
- No Surprises Act training video playlist: YouTube Playlist
- No Surprises Act Toolkit: https://www.cms.gov/nosurprises/consumer-advocate-toolkit

Appendix B. Warning and Security & Privacy Agreement

The warning and privacy statements outline the rules for using the IDR Gateway responsibly and protecting information to ensure proper use, safeguard data, and create a secure and reliable environment for all users.

WARNING:

This system contains U.S. Government Data and is only available to users in the U.S. and its territories. Unauthorized use of this system is prohibited.

The Independent Dispute Resolution (IDR) Gateway is provided only for authorized use by participants in the Federal IDR process. All information, documentation, and communications that are submitted by stakeholders in the IDR Gateway are only for authorized U.S. Government and certified IDR entity use. U.S. Government computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized U.S. Government entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Use of this system implies understanding of these terms and conditions.

*** You Must Read and Agree to the Security & Privacy Agreement:**

By using web forms, we provide for use in connection with the Federal Independent Dispute Resolution (IDR) process, you agree to the collection and use of information as described in this Privacy Act Statement.

The Centers for Medicare & Medicaid Services (CMS) ("us," "we," or "our") manages the forms used by parties to start payment disputes available on https://nsa-idr.cms.gov/paymentdisputes. Users may submit the forms electronically by completing the “Notice of IDR Initiation” web form. The information on this page tells you about our policies regarding the collection, use, and disclosure of personal information we receive from users of the web forms. It also includes specifics about personal information and other information that may be collected about you. A separate IDR Website Privacy Policy provides more information about CMS website privacy information for the Federal IDR portal, which you should also read and be aware of how information is collected and used when on the Federal IDR portal.

Permission for information submitted on IDR web forms

When submitting any Federal IDR web forms, you also represent that you are authorized to submit the web form, as well as to receive any communications about the payment dispute, its status, or a final decision related to the payment dispute. For example, if you submit the “Notice of IDR Initiation” web form, you represent that you are authorized to start the dispute on behalf of the health care provider, health care facility, provider of air ambulance services, group health plan, health insurance issuer, or Federal Employees Health Benefits (FEHB) carrier, as applicable, regarding any related claim(s) for the qualified IDR item(s) and/or service(s) to the participant’s, beneficiary’s, or enrollee’s plan.

CMS.gov Privacy Policy

Protecting your privacy is very important to us. This privacy policy describes what information we collect, why we collect it, and what we do with it, available at https://www.cms.gov/privacy.

Federal Independent Dispute Resolution Process Privacy Act Statement – effective August 14, 2026

The Departments of the Treasury, Labor, and Health and Human Services (HHS) (collectively, the Departments), and the Office of Personnel Management (OPM) are authorized to collect the information on submitted web forms and any supporting documentation under Internal Revenue Code sections 9816(c) and 9817(b), ERISA sections 716(c) and 717(b), PHS Act sections 2799A-1(c) and 2799A-2(b), and 5 U.S.C. 8902(p). This law directs the Departments and OPM to establish a process to restrict surprise billing for participants, beneficiaries, and enrollees of group health plans, health insurance issuers offering group or individual health insurance coverage, and FEHB carriers who receive emergency services from nonparticipating health care providers or health care facilities, non-emergency services from nonparticipating health care providers at participating health care facilities, and air ambulance services from nonparticipating health care providers of air ambulance services.

We need the information provided about parties to the Federal IDR process to manage Notices of IDR Initiation and to otherwise support resolution of payment disputes and our oversight of the Federal IDR process. Do not include personally identifiable information (PII) or protected health information (PHI) in the payment dispute web form submissions unless specifically requested. The information collected through the payment dispute web forms will be used to verify the eligibility of disputes for the Federal IDR process and to resolve payment disputes. The Departments have established access to administer the Federal IDR process, available at https://www.cms.gov/nosurprises.

The initiating party must furnish the Notice of IDR Initiation to the Departments by submitting the notice through the Independent Dispute Resolution web page. The contact information provided on the "Notice of IDR Initiation" web form will be used to send the parties a notice identifying and/or confirming the certified IDR entity assigned to the dispute. This information will be shared with the certified IDR entity for consideration and for the purpose of enabling the certified IDR entity to make eligibility and payment determinations. We will also use the information as part of the ongoing operation of the Federal IDR process, including managing and reporting on the Federal IDR process, and performing oversight and quality control activities in relation to certified IDR entities. We may also use the information to evaluate whether a certified IDR entity or its staff have any conflicts of interest that would preclude it from making a payment determination. The information may further be used to combat fraud and noncompliance within the Federal IDR process and respond to any concerns about the security or confidentiality of the information.

Providing the requested information is voluntary. If any plan, issuer, FEHB carrier, health care provider, health care facility, or provider of air ambulance services, or any third-party administrator knowingly fails to provide correct information on submitted web forms or knowingly and willfully provides false or fraudulent information, they may be subject to penalties and other enforcement actions.

To manage disputes within the Federal IDR process, we will need to share certain information with people or entities outside of CMS, and may include:

1. A certified IDR entity, which we have certified to make payment determinations. The certified IDR entity will only use this information for the purpose of making payment determinations;
2. Contractors engaged to perform functions related to or in support of the Federal IDR process, including contractors that will support the payment of certified IDR entity fees and administrative fees;
3. Business Associates and other authorized entities who have executed appropriate agreements and maintain compliance with federal privacy and security requirements;

4. All parties to a dispute and their authorized representatives;
5. Other federal agencies that are responsible for implementing and overseeing plans that are subject to the Federal IDR process, including the Departments and OPM; and
6. Anyone else as required by law or allowed under the Privacy Act System of Records Notice associated with this collection entitled, "Complaints Against Health Insurance Issuers and Health Plans (CAHII)," System No. 09-70-9005, 66 FR 9858 (Feb. 12, 2001), as amended, 83 FR 6591 (Feb. 14, 2018).

Recipients must comply with federal confidentiality requirements and implement required security measures. This statement provides the notice required by the Privacy Act of 1974 (5 U.S.C. § 552a(e)(3)). You can learn more about how we handle your information at: https://www.cms.gov/nosurprises/privacy.

Security Safeguards:

1. This system implements administrative, technical, and physical safeguards consistent with federal standards, including the Federal Information Security Modernization Act (FISMA) and The National Institute of Standards and Technology (NIST) guidance, and CMS Information Security and Privacy policies.
2. This statement provides the notice required by the Privacy Act of 1974 (5 U.S.C. 552a(e)(3)). Learn more at https://www.cms.gov/nosurprises/privacy.

Contact Us

If you have any questions about this Privacy Act Statement, please contact us at Privacy@cms.hhs.gov.

Appendix C. IDR Gateway Rules of Behavior

These *Rules of Behavior (RoB) for IDR Gateway Users* apply to all users who are granted access to Federal IDR process information, resources, and IT systems through the IDR Gateway. The IDR Gateway provides parties with a mechanism to engage with, track, and manage IDR payment disputes, including the submission of required information to start a dispute and upload of associated documents through web forms (e.g., Notice of Initiation [NOI], Selection/Reselection Response, and Notice of Offer [NOOF]) within a sign-in community. Users of the IDR Gateway must read, acknowledge, and adhere to the following rules prior to accessing data and/or documents and using the IDR Gateway.

A. The IDR Gateway

When using and accessing the IDR Gateway, I understand that I must:

1. Comply with federal laws, regulations, and the IDR Gateway policies, standards, and procedures and that I must not violate, direct, or encourage others to violate these policies, standards, or procedures. Not allow unauthorized use and access to the IDR Gateway information and resources. Not access the IDR Gateway information and resources outside the U.S. and its territories.
2. Not circumvent or bypass security safeguards, policies, systems' configurations, or access control measures unless authorized in writing.
3. Review all the IDR Gateway user guides when initially granted access to the IDR Gateway and periodically thereafter as required by Federal IDR policies.
4. Be accountable for my actions while accessing and using the IDR Gateway information and information systems.
5. Sign out of the IDR Gateway whenever not actively working within it.
6. Not enter personally identifiable information (PII) or personal health information (PHI) in any fields in the IDR Gateway. This includes, but is not limited to, patient names, social security numbers, medical record numbers, health plan beneficiary numbers, and any other unique identifying characteristics as defined by the Privacy Act of 1974 and HIPAA Privacy Rule.
7. Redact any PII/PHI from documents before uploading them to the IDR Gateway. This includes reviewing all attachments, embedded content, and metadata to ensure complete removal of sensitive information in accordance with HIPAA Privacy Rule requirements, Privacy Act provisions, and the National Institute of Standards and Technology (NIST) SP 800-88 Rev. 2, Guidelines for Media Sanitization.
8. Understand that unauthorized disclosure of PII/PHI may result in violations of both the Privacy Act of 1974 and HIPAA regulations, potentially leading to civil and criminal penalties.
9. Implement appropriate administrative, technical, and physical safeguards to protect any sensitive information that may be accessed through the IDR Gateway.
10. Report all suspected and identified information security incidents and privacy breaches to FederalIDRQuestions@cms.hhs.gov as soon as possible, without unreasonable delay and no later than within one (1) hour of occurrence/discovery. This reporting requirement applies to any potential exposure of PII/PHI, regardless of the circumstance or scale of the incident.

B. No Expectation of Privacy

When using and accessing the IDR Gateway information and systems, I understand that I would have no expectation of privacy. I acknowledge there would be no expectation of privacy when using the IDR Gateway information, resources, and systems and activity within the IDR Gateway may be monitored, recorded, and audited at any time.

C. Password Requirement

When creating and managing my password, I understand that I must comply with the following baseline requirements:

1. Comply with all of the IDR Gateway's password requirements.
2. Create passwords with minimum of 15 characters.
3. Not use common or compromised passwords.
4. Protect my passwords and other access credentials from disclosure and compromise.
5. Promptly change my password if I suspect or receive notification that it has been compromised.
6. Immediately select a new password upon account recovery.
7. Not use another person's account, identity, password, or allow others to use my account to access the IDR Gateway. This includes not sharing passwords or providing passwords to anyone, including system administrators.
8. Only use authorized credentials to access the IDR Gateway and will not attempt to bypass access control measures.

SIGNATURE

I have read the above *Rules of Behavior for IDR Gateway Users* and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or the IDR Gateway's information, security policies, and standards may result in suspension of access privileges, revocation of access to the IDR Gateway, deactivation of accounts, monetary fines, removal or debarment from work on federal contracts or projects, and/or criminal charges that may result in imprisonment.

I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing officials. I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 U.S.C. 2071, which the IDR Gateway RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

If you have any questions about this *Rules of Behavior for IDR Gateway Users*, please contact us at IDRGatewayHelp@cms.hhs.gov.

I have read and agree to comply with *Rules of Behavior for IDR Gateway Users*.

Appendix D. Acronyms & Terms

The following acronyms and terms are used in this user guide and throughout the IDR Gateway.

Acronym/Term	Definition
Access Type	The IDR Gateway offers two user access types: verified and administrator.
Credential Service Provider	A credential service provider is a trusted entity whose functions include identity proofing applicants and registering authenticators to subscriber accounts. A credential service provider may be an independent third party.
CMS	Centers for Medicare & Medicaid Services
FEHB	Federal Employees Health Benefits
HHS	Department of Health and Human Services
IDM	Identity Management
IDR	Independent Dispute Resolution
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
NSA	No Surprises Act
PHI	Personal Health Information
PII	Personally Identifiable Information
Role	The IDR Gateway offers three user access roles controlled by the organization administrator: view only, initiation and selection roles, and full access roles.
SSN	Social Security Number
the Departments	The Department of Health and Human Services, the Department of Labor, and the Department of the Treasury
TPA	Third-Party Administrator
Workspace	Workspaces are secure spaces organizations use to grant or restrict access to disputes based on the email addresses assigned to the workspace.

This communication was printed, published, or produced
and disseminated at U.S. taxpayer expense.