EMERGENCY MEDICAL SERVICES AND TRAUMA REGISTRIES

REQUESTING A NEW EMSTR USER ACCOUNT

TEXAS
Health and Human
Services

Texas Department of State
Health Services

Emergency Medical Services and Trauma Registries

Job Aid for:

Registry Users who need to Create an EMSTR User Account

Contents

Overview:

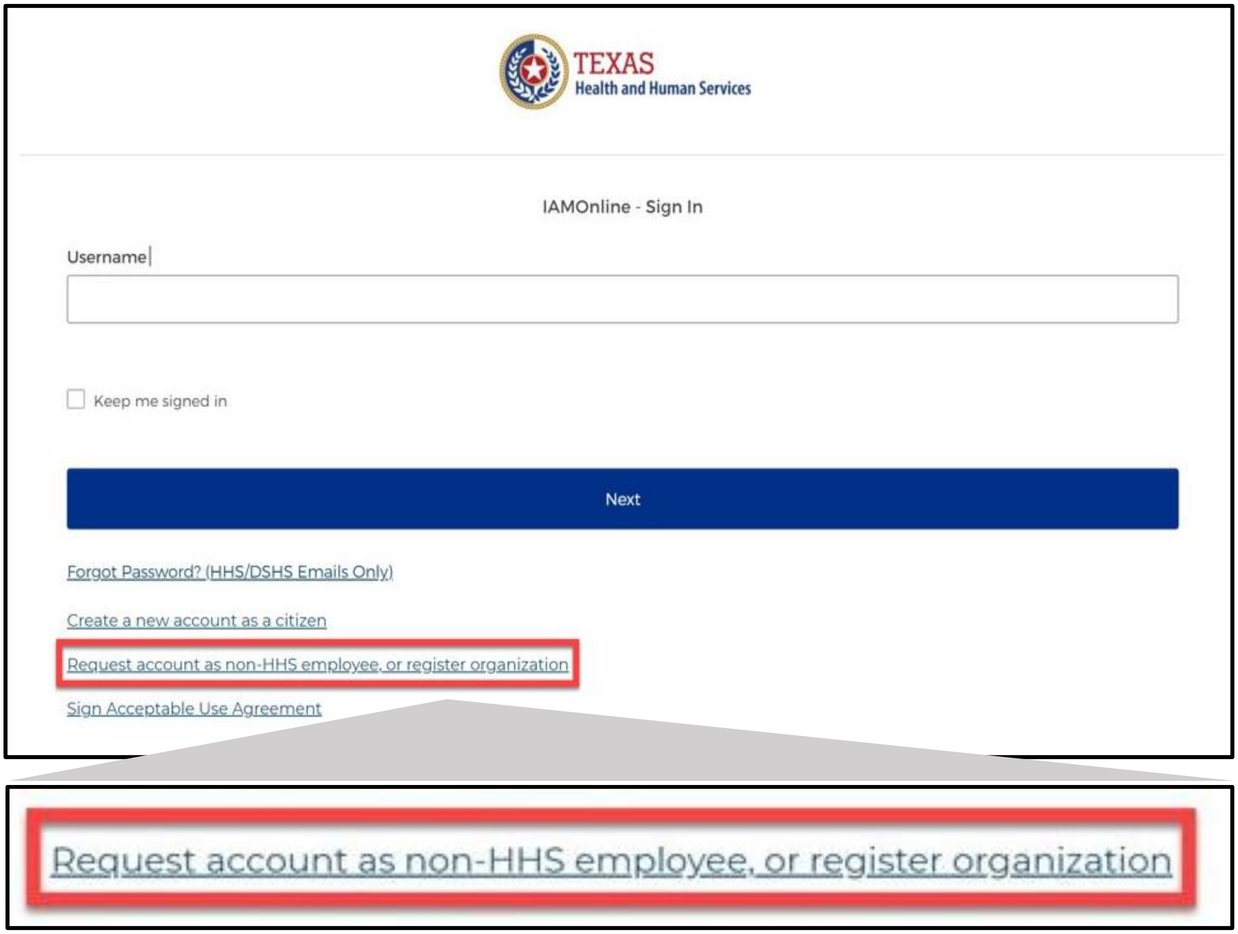
This job aid is for users who need an account to access the Texas Department of State Health Services (DSHS) Emergency Medical Services and Trauma Registries (EMSTR) application. It provides step-by-step instructions on how to request an account associated with your facility, activate your account, set-up security methods, access the MyApps dashboard, request EMSTR access, and access EMSTR.

If you are a facility organization administrator who needs to register your facility, please access the “How to Register a New Facility” **here**.

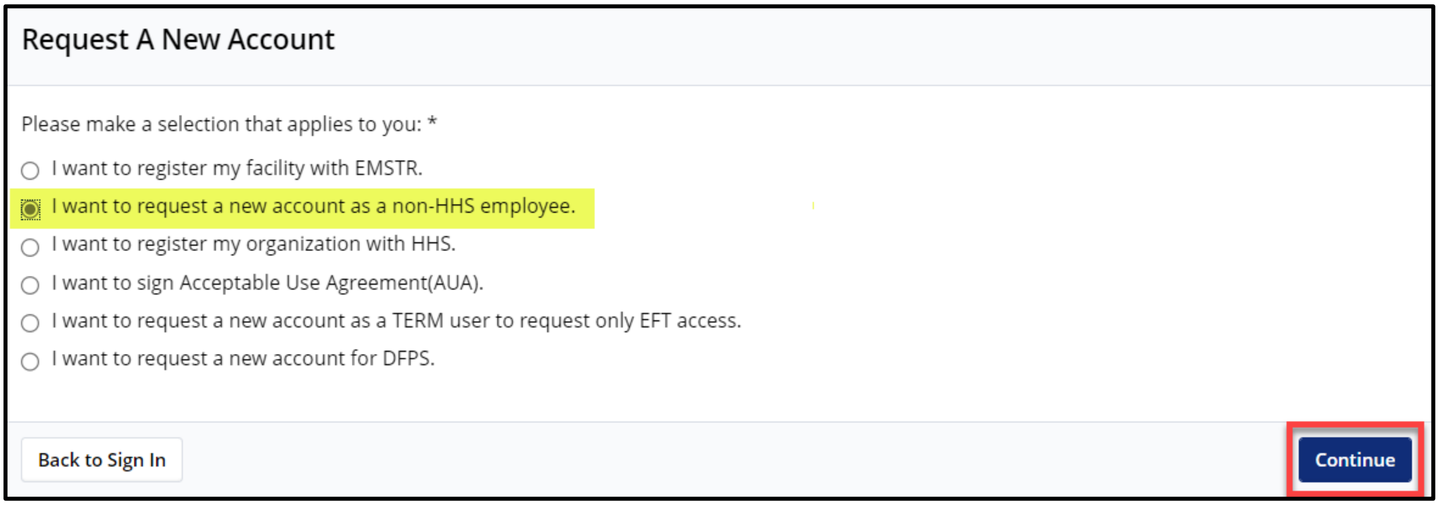
Step 1: Request an Account

Before you request an account, you will need either the **name of your organization**, exactly how it is spelled out in the new DSHS Identity and Access Management Online (IAMOnline) system, or your **Employee Identification Number (EIN)**. If you do not have this information, please reach out to your facility administrator. All users working with Texas Health and Human Services (HHS) programs will need to request an account.

- To request a new EMSTR account associated with your facility, access the **IAMOnline sign-in page**.
- Select **"Request account as non-HHS employee or register organization"**.


TEXAS
Health and Human Services
IAMOnline - Sign In
Username
□ Keep me signed in
Next
Forgot Password? (HHS/DSHS Emails Only)
Create a new account as a citizen
Request account as non-HHS employee, or register organization
Sign Acceptable Use Agreement
Request account as non-HHS employee, or register organization

- After selecting **Request account as non-HHS employee or register organization**, click the **"I want to request a new account as a non-HHS employee"** option.
- Select the **"Continue"** button.



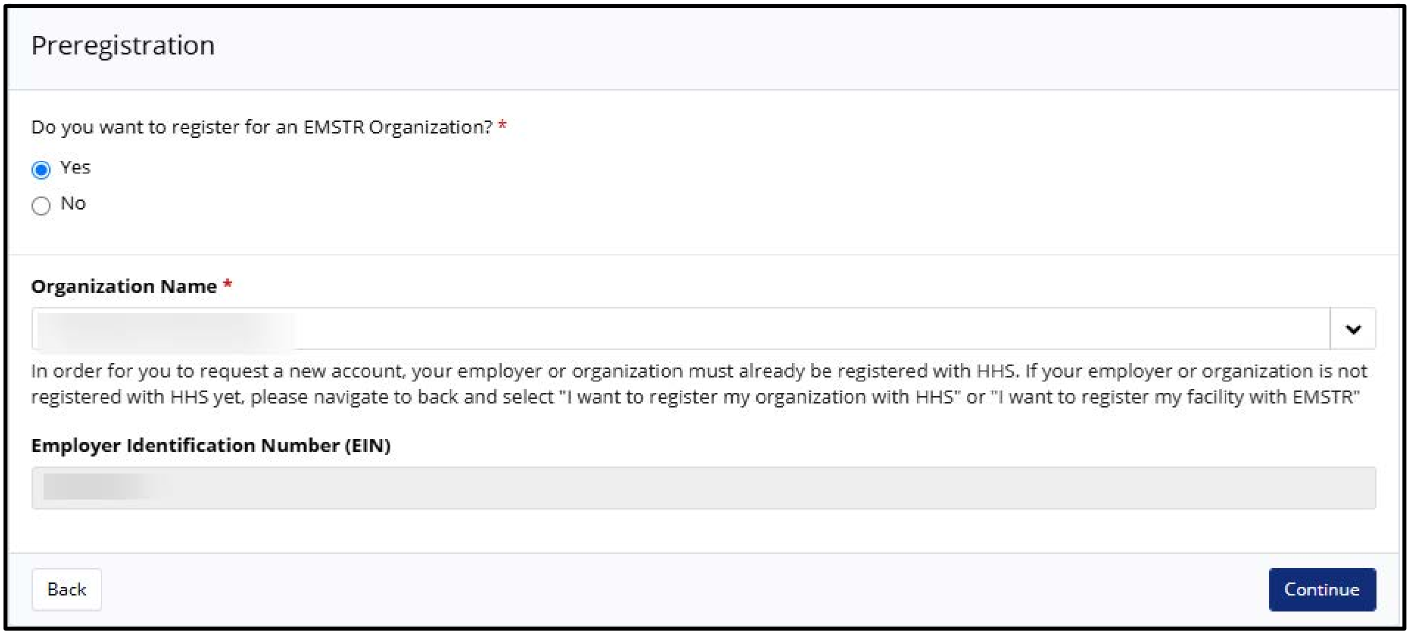
Request A New Account

Please make a selection that applies to you: *

○ I want to register my facility with EMSTR.
● I want to request a new account as a non-HHS employee.
○ I want to register my organization with HHS.
○ I want to sign Acceptable Use Agreement(AUA).
○ I want to request a new account as a TERM user to request only EFT access.
○ I want to request a new account for DFPS.

- Confirm you want to register for an EMSTR Organization by selecting the **"Yes"** on the Preregistration section.
- Enter your **Organization Name and DSHS ID** in the **EIN or Organization Name** field.
  - Example—*Hospital of City 123456*
  - The administrator can confirm this information through their IAMOnline account. Refer to slides 49-53 on the administrator guide.

- Select the **"Continue"** button after completing the Preregistration section.



Preregistration

Do you want to register for an EMSTR Organization? *

● Yes
○ No

Organization Name *

[redacted]

In order for you to request a new account, your employer or organization must already be registered with HHS. If your employer or organization is not registered with HHS yet, please navigate to back and select "I want to register my organization with HHS" or "I want to register my facility with EMSTR"

Employer Identification Number (EIN)

[redacted]

Complete the Partner User Registration Form

Complete the Partner User Registration form's required fields indicated by red asterisks (*). The required fields are listed below:

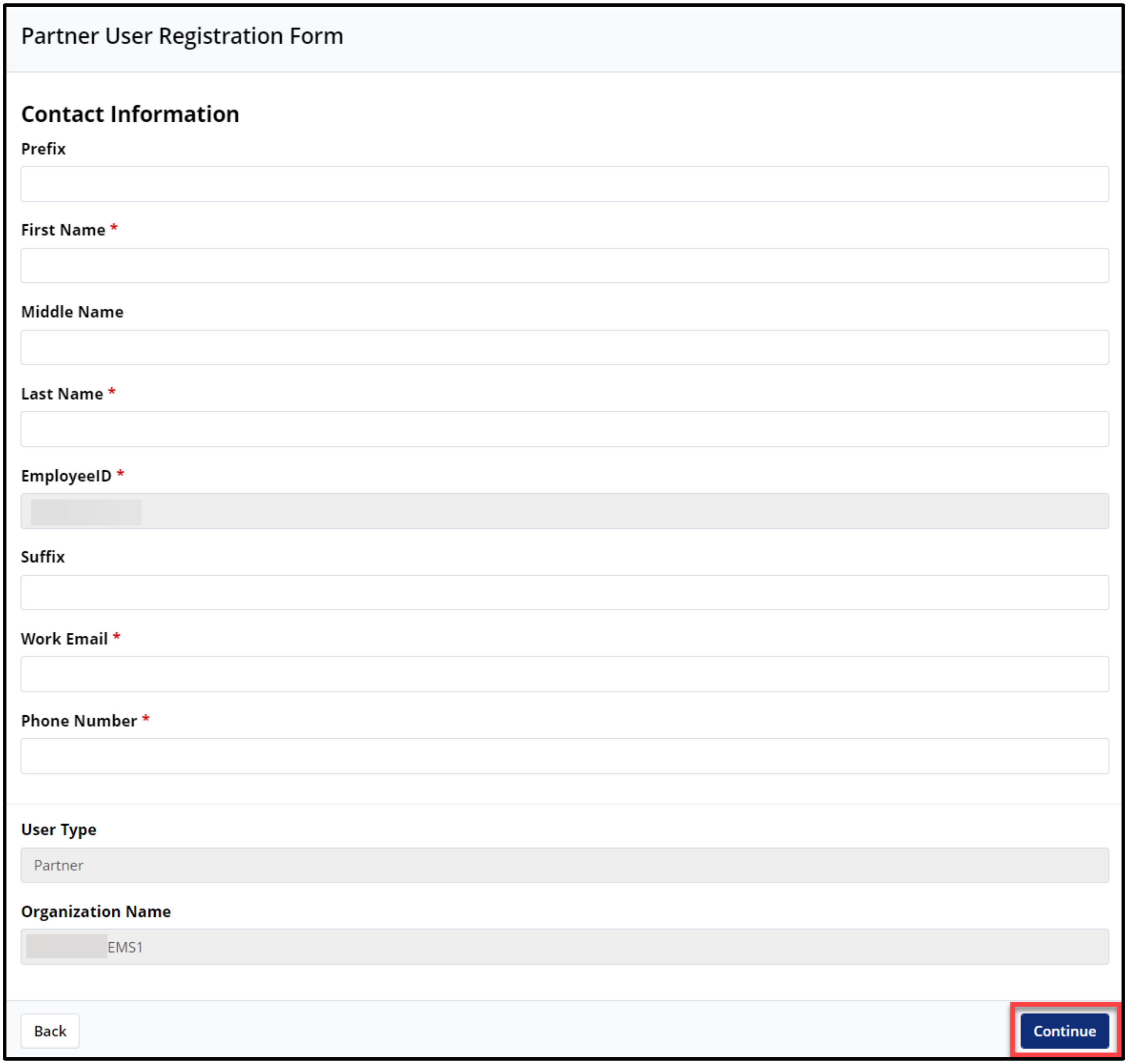
- **First Name;**
- **Last Name;**
- **EmployeeID –** Enter your unique employee identification number from your facility;
- **Work Email –** Enter your employee email address for your facility; and
- **Phone Number.**

Auto-generated fields:

- **User Type –** The type of user you are categorized in the IAMOnline system.
- **Organization Name –** The name of your facility.

After completing the required fields, select the **"Continue"** button.

Example of the **Partner User Registration Form**:



Partner User Registration Form

Contact Information

Prefix

First Name *

Middle Name

Last Name *

EmployeeID *

[redacted]

Suffix

Work Email *

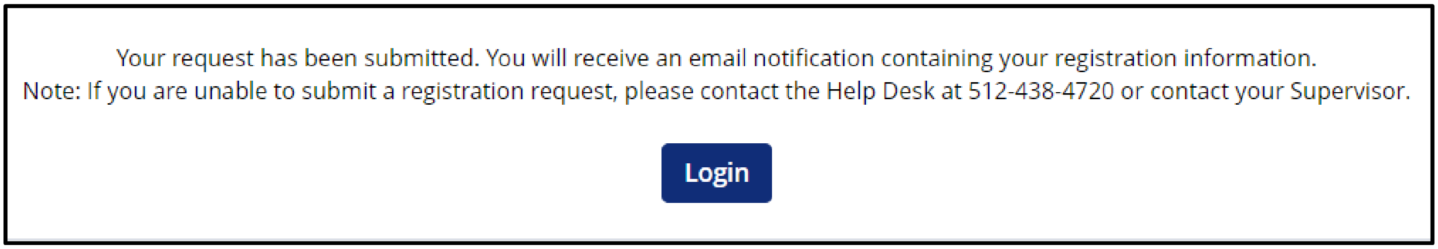
Phone Number *

User Type

Partner

Organization Name

[redacted] EMS1



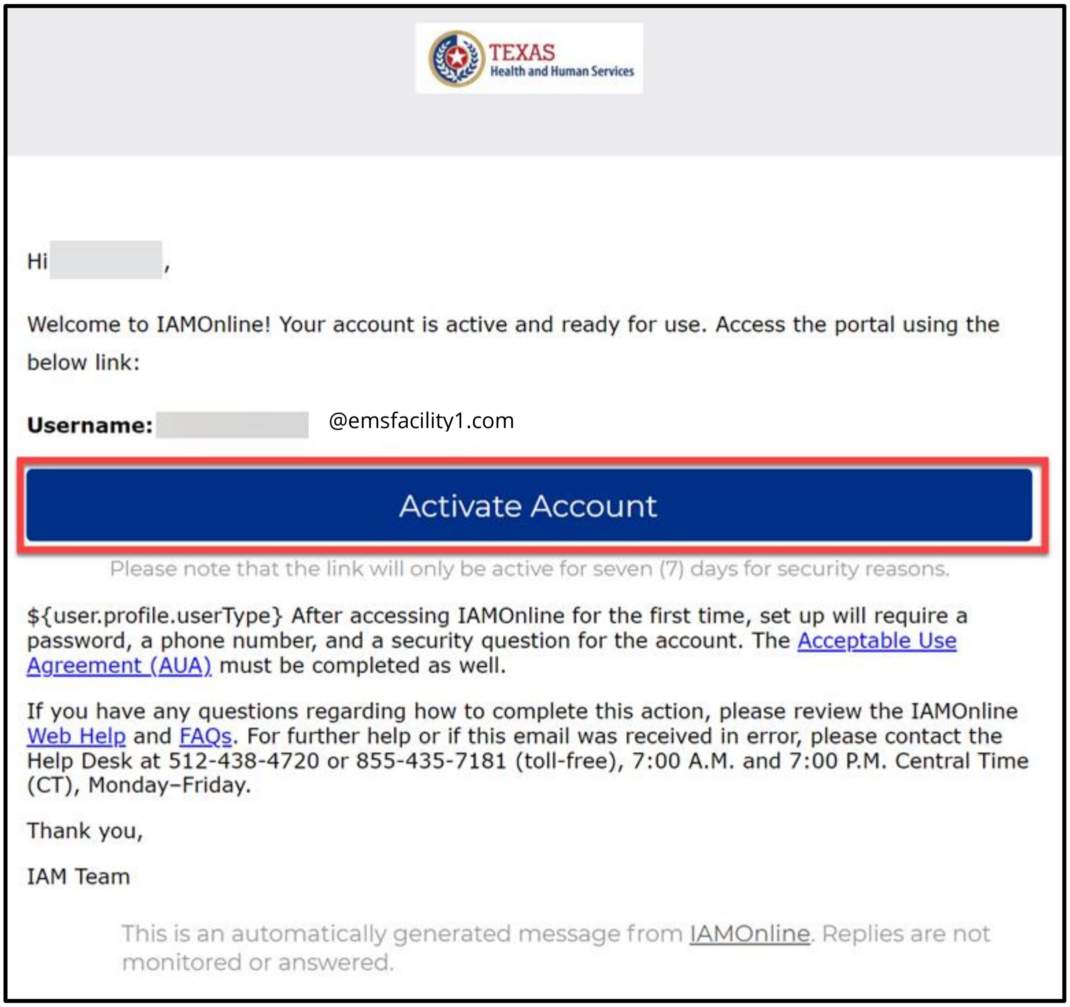
Your request has been submitted. You will receive an email notification containing your registration information.
Note: If you are unable to submit a registration request, please contact the Help Desk at 512-438-4720 or contact your Supervisor.

- After submitting the **Organization Registration Form**, your facility organization administrator will review your request.
- If your facility organization administrator approves the request, you will receive an activation email.
- If your facility organization administrator denies your request, please contact them directly for next steps.
- Re-submit the request if needed.

Step 2: Activate your Account

To activate your account, find the **noreply@okta.com** email in your employee email inbox. Check your junk folder if you do not find it in your inbox. Click the **“Activate Account”** button.

Note – This link will only be active for **seven (7) days** from receipt of the email for security purposes.



Hi [redacted],

Welcome to IAMOnline! Your account is active and ready for use. Access the portal using the below link:

Username: [redacted] @emsfacility1.com

Please note that the link will only be active for seven (7) days for security reasons.

${user.profile.userType} After accessing IAMOnline for the first time, set up will require a password, a phone number, and a security question for the account. The Acceptable Use Agreement (AUA) must be completed as well.

If you have any questions regarding how to complete this action, please review the IAMOnline Web Help and FAQs. For further help or if this email was received in error, please contact the Help Desk at 512-438-4720 or 855-435-7181 (toll-free), 7:00 A.M. and 7:00 P.M. Central Time (CT), Monday–Friday.

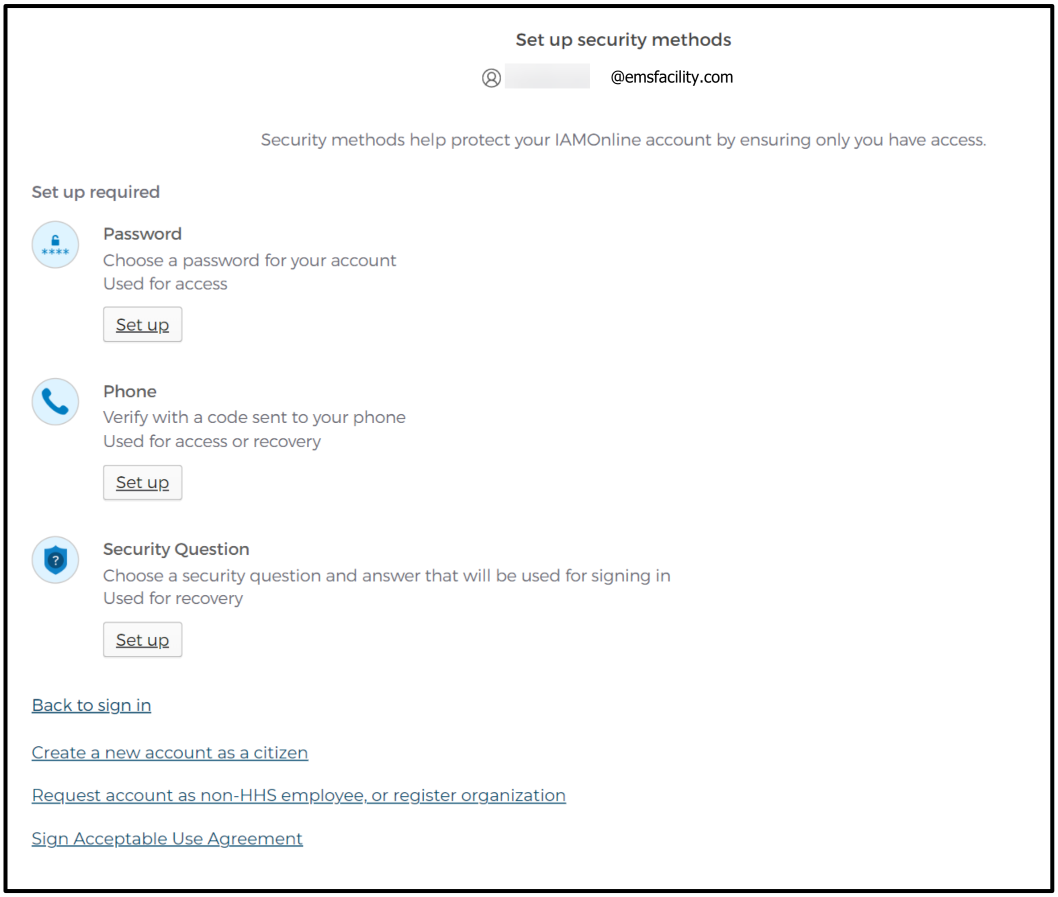
Thank you,

IAM Team

This is an automatically generated message from IAMOnline. Replies are not monitored or answered.

Step 3: Set up security methods

After selecting **Activate Account**, the system will immediately prompt you to set up your security methods to protect your account with a **Password**, your **Phone**, and a **Security Question**. This is known as multifactor authentication (MFA).



Set up security methods

@emsfacility.com

Security methods help protect your IAMOnline account by ensuring only you have access.

Set up required

Password
Choose a password for your account
Used for access

Set up

Phone
Verify with a code sent to your phone
Used for access or recovery

Set up

Security Question
Choose a security question and answer that will be used for signing in
Used for recovery

Set up

Back to sign in

Create a new account as a citizen

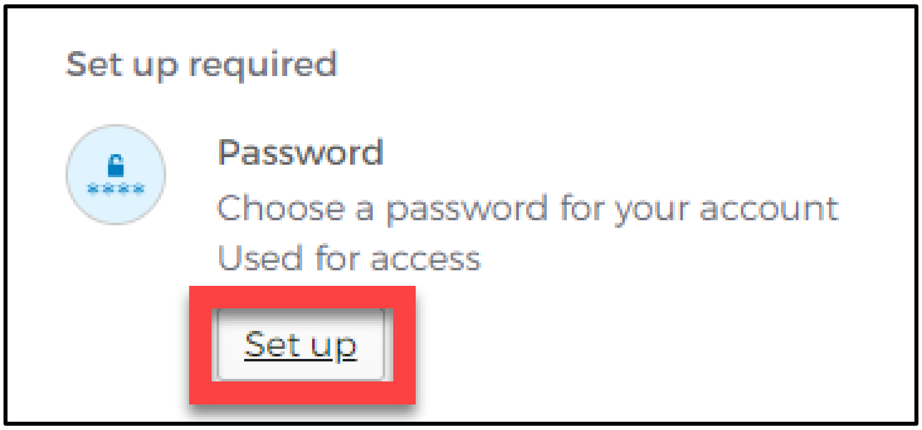
Request account as non-HHS employee, or register organization

Sign Acceptable Use Agreement

Password

You need a password to access the account as the new DSHS IAMOnline system provides a single sign-on to all HHS applications.

To set up a **Password**, click the **"Set up"** button.



Set up required

Password

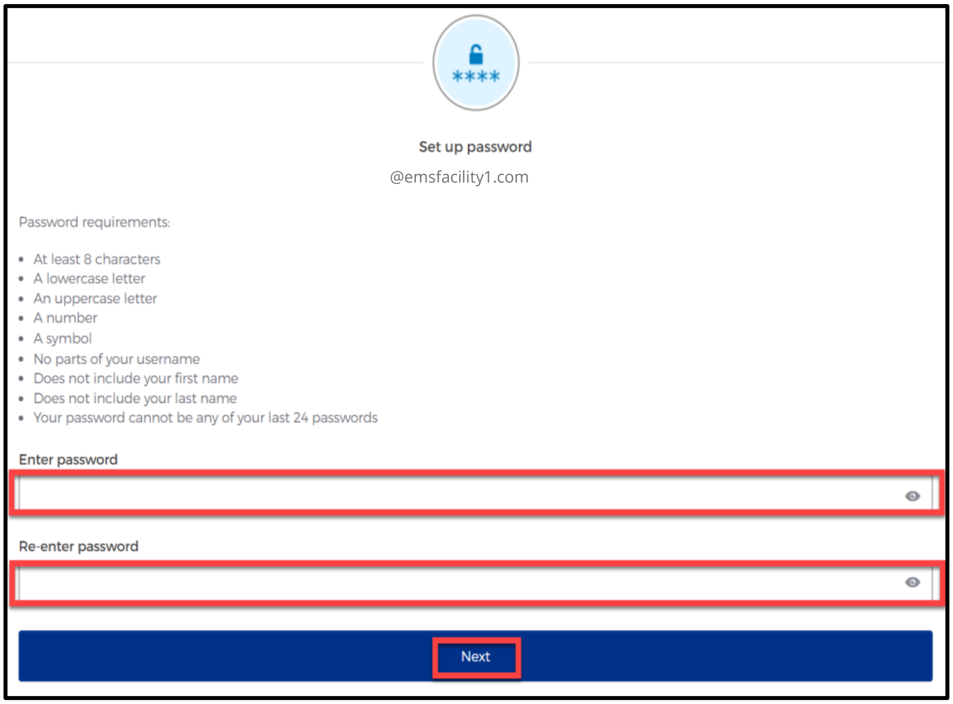
Choose a password for your account

Used for access

You must create a password that meets all HHS requirements listed below:

- At least eight (8) characters in length;
- A lowercase letter;
- An uppercase letter;
- A number;
- A symbol;
- Does not include any parts of the user's username;
- Does not include the user's first name;
- Does not include the user's last name;
- The password cannot be any of the user's previous six (6) passwords; and
- At least one (1) day must have passed since you last changed your password.

Example of the **Set up password** screen:



Set up password

@emsfacility1.com

Password requirements:

- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 24 passwords

Enter password

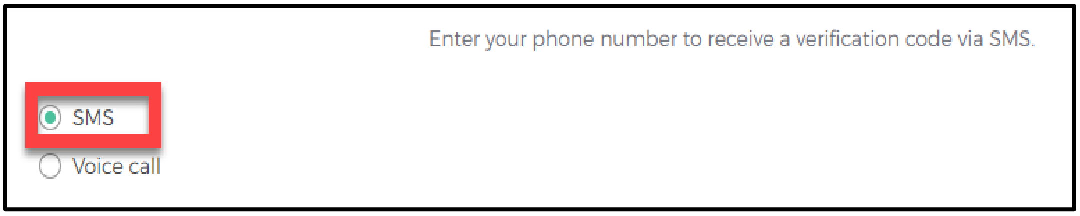
Re-enter password

- Create a new password by typing it in the **“Enter password”** text box and re-entering it in the **“Re-enter password”** text box.
- Click the **“Next”** button.
  - **Tip –** Click the password reveal icon to see the typed text. 👁
  - **Tip –** If an error message appears, re-read the password requirements and create a different password.

Phone Number

To set up your phone number, select the **“SMS”** (short messaging service or text message) or **“Voice call”** option. The **SMS** option will send a text message to your phone and the **Voice call** option will send an automated call. The phone number must be a valid U.S. number.

Example of SMS option selected.



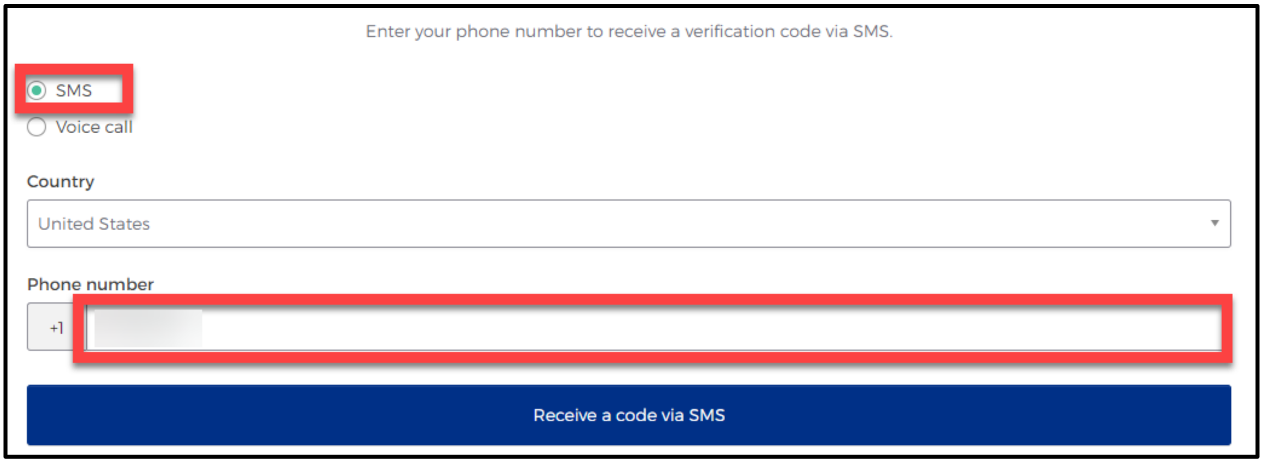
Enter your phone number to receive a verification code via SMS.

● SMS
○ Voice call

Short Messaging Service (SMS)

Use your phone number to verify the account. The automated system will send a verification code to your phone number via **SMS**.

- The **Country** code must be for the **United States** (+1).
- Type your ten-digit **Phone number** in the text box. This phone number must be able to receive an SMS. *Carrier messaging charges may apply*.
- Click the **“Receive a code via SMS”** button.



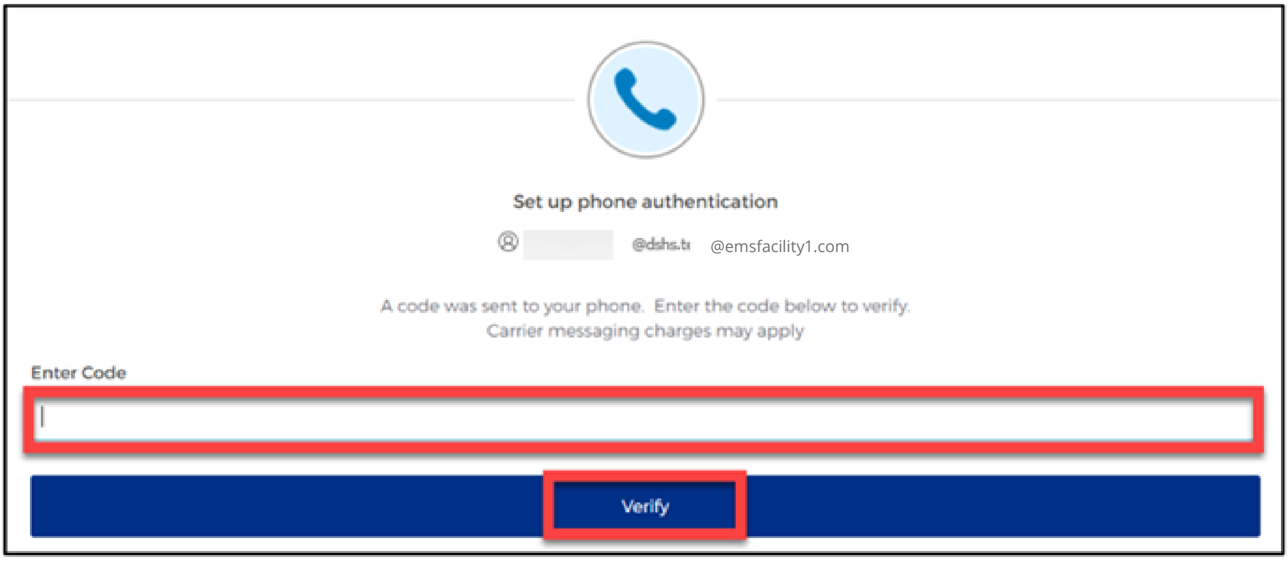
Enter your phone number to receive a verification code via SMS.

● SMS
○ Voice call

Country
United States

Phone number
+1 [redacted]

The system will send an automated code to the listed phone number via SMS.



Set up phone authentication

[redacted] @dshs.t @emsfacility1.com

A code was sent to your phone. Enter the code below to verify.
Carrier messaging charges may apply

Enter Code

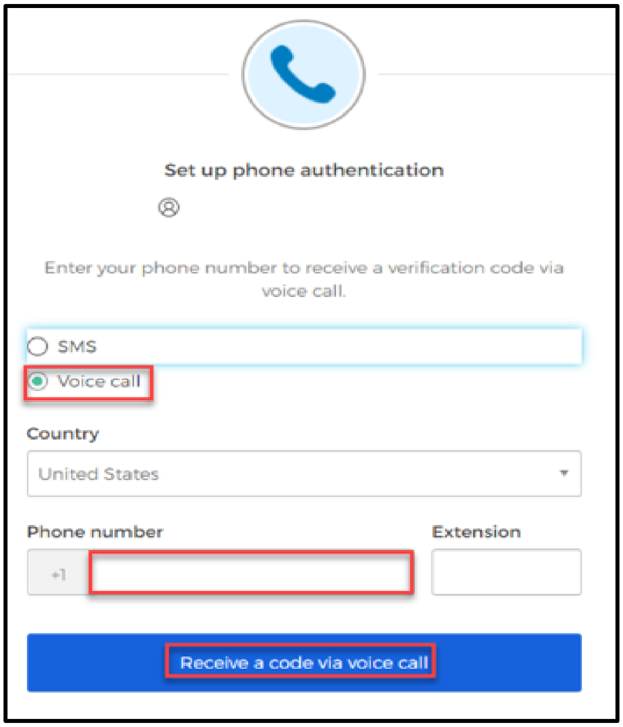
Verify

Type the code you receive in the text box and click the **"Verify"** button.

Voice Call

The second option to verify the account is a voice call. The system can provide an automated **verification code** via **Voice call**.

- The **Country** must be for the **United States** (+1).
- Type your ten-digit **Phone number** in the text box to receive a code by voice call.
- Click the **"Receive a code via voice call"** button.



Set up phone authentication

Enter your phone number to receive a verification code via voice call.

○ SMS
● Voice call

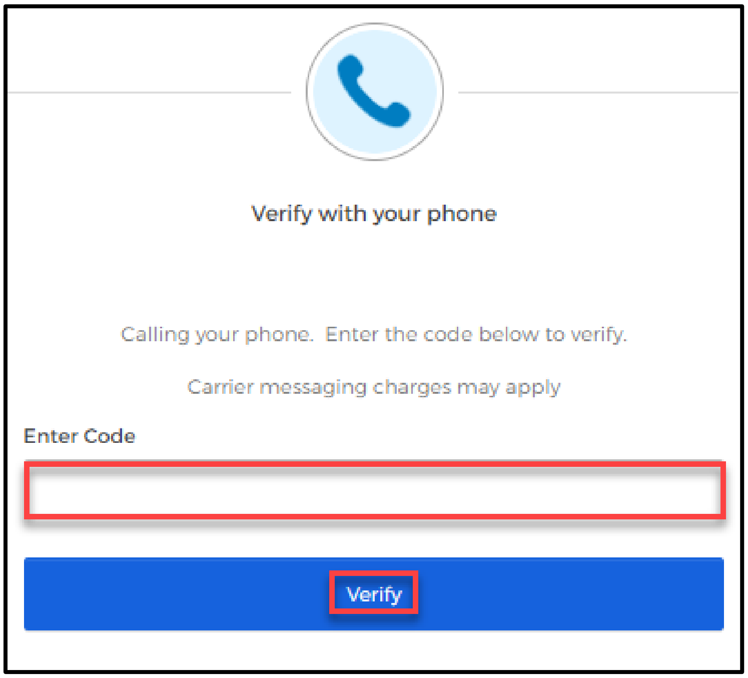
Country: United States

Phone number: +1

Extension:

Receive a code via voice call

- Type the code provided by the voice call in the **Enter Code** text box and click the **“Verify”** button.



Verify with your phone

Calling your phone. Enter the code below to verify.

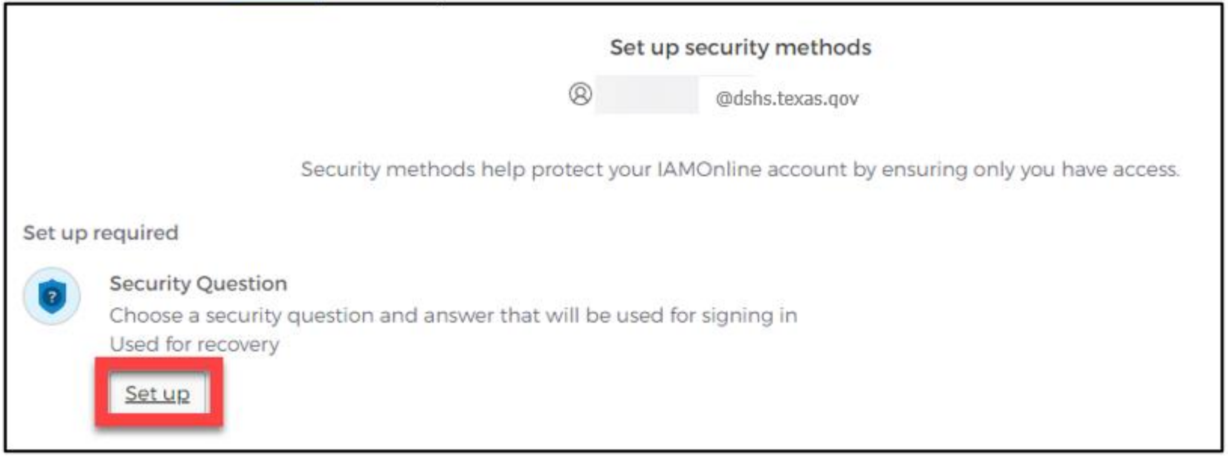
Carrier messaging charges may apply

Enter Code

Security Question

Set up a security question to protect the account.

- Click the **“Set up”** button.



Set up security methods

[redacted]@dshs.texas.qov

Security methods help protect your IAMOnline account by ensuring only you have access.

Set up required

Security Question

Choose a security question and answer that will be used for signing in

Used for recovery

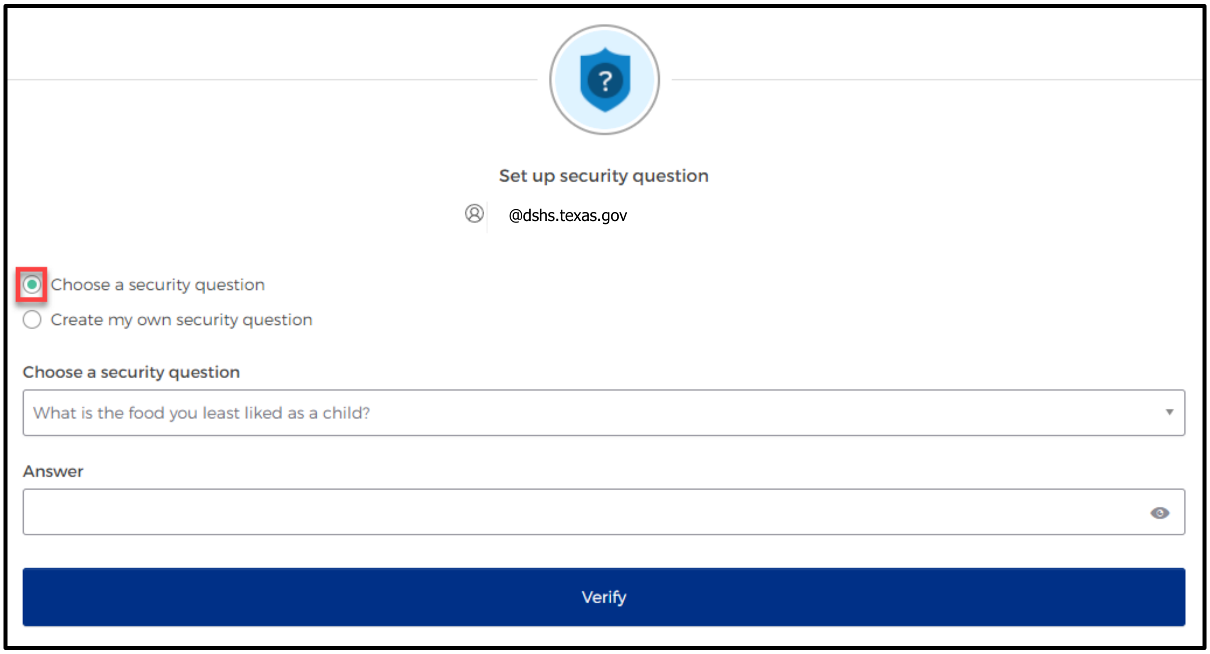
You can either **Choose a security question** or **Create my own security question**.

Creating your own security question

- If creating a security question, create one that cannot be guessed by others, even those who know you well, for security purposes.
- Type your answer in the **“Answer”** box.

Choosing a security question

- To choose a security question, select the **“Choose a security question”** option.



Set up security question

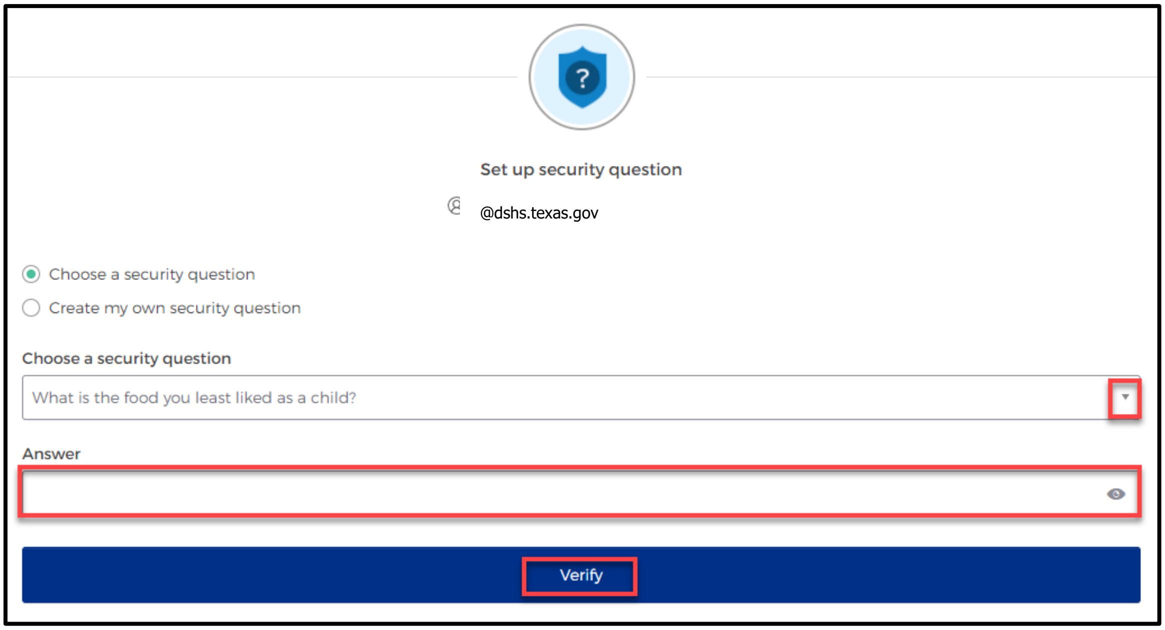
@dshs.texas.gov

● Choose a security question
○ Create my own security question

Choose a security question: What is the food you least liked as a child? ▾

Answer

- Select the “**Drop-down Icon”** ▼ and scroll to select a security question.
- Type your answer in the **“Answer”** box.
- After selecting a secuirty question and typing in your answer, select the **“Verify”** button.



Set up security question

@dshs.texas.gov

● Choose a security question

○ Create my own security question

Choose a security question

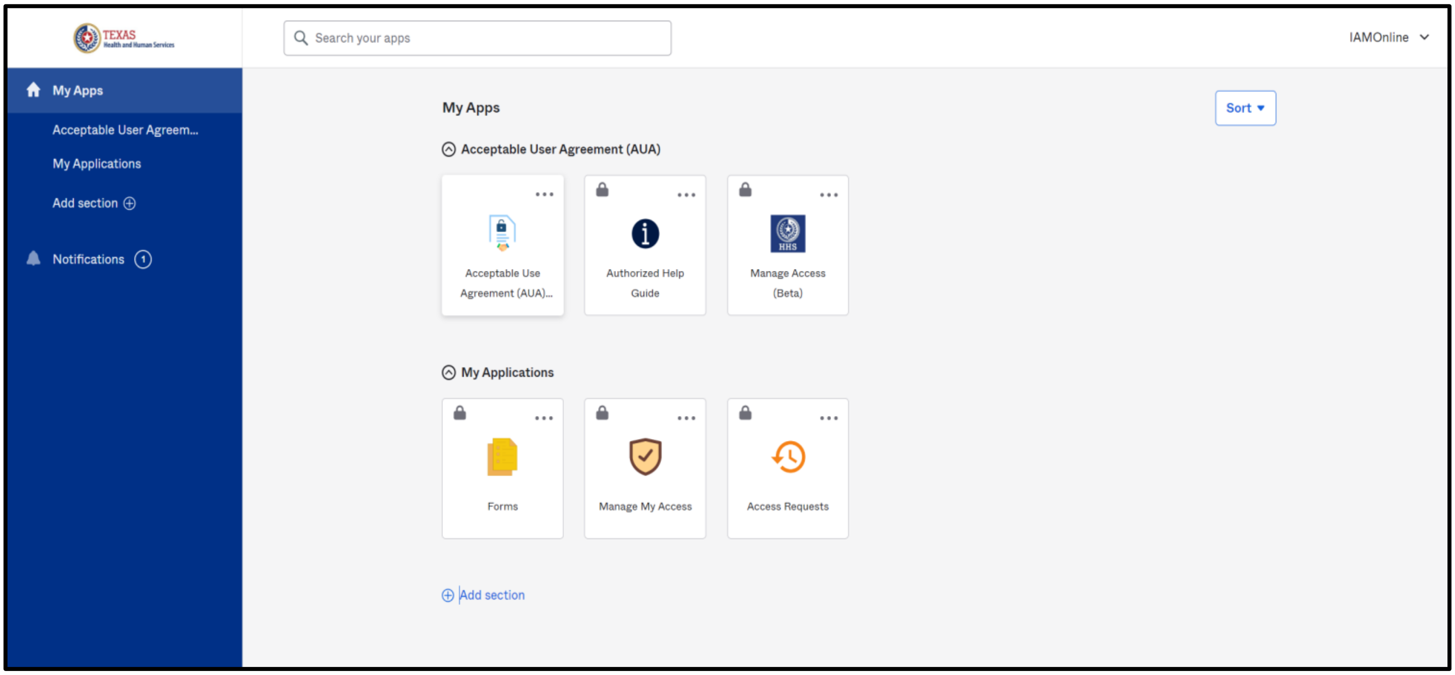
What is the food you least liked as a child?

Answer

Step 4: Access the MyApps Dashboard

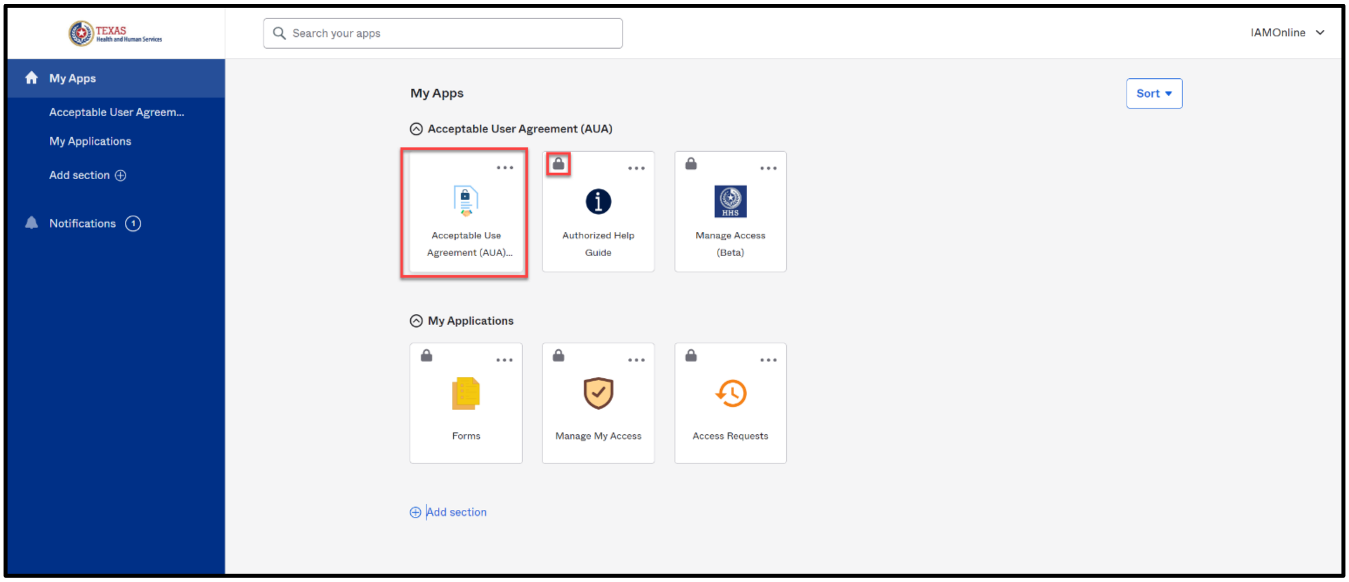
Your account set up is now complete and you can access your **My Apps** dashboard.

- This centralized dashboard holds applications, systems, and software in one place for the user to easily access and use.
- IAMOnline will also allow you to request and easily manage EMSTR access.



Acceptable Use Agreement (AUA)

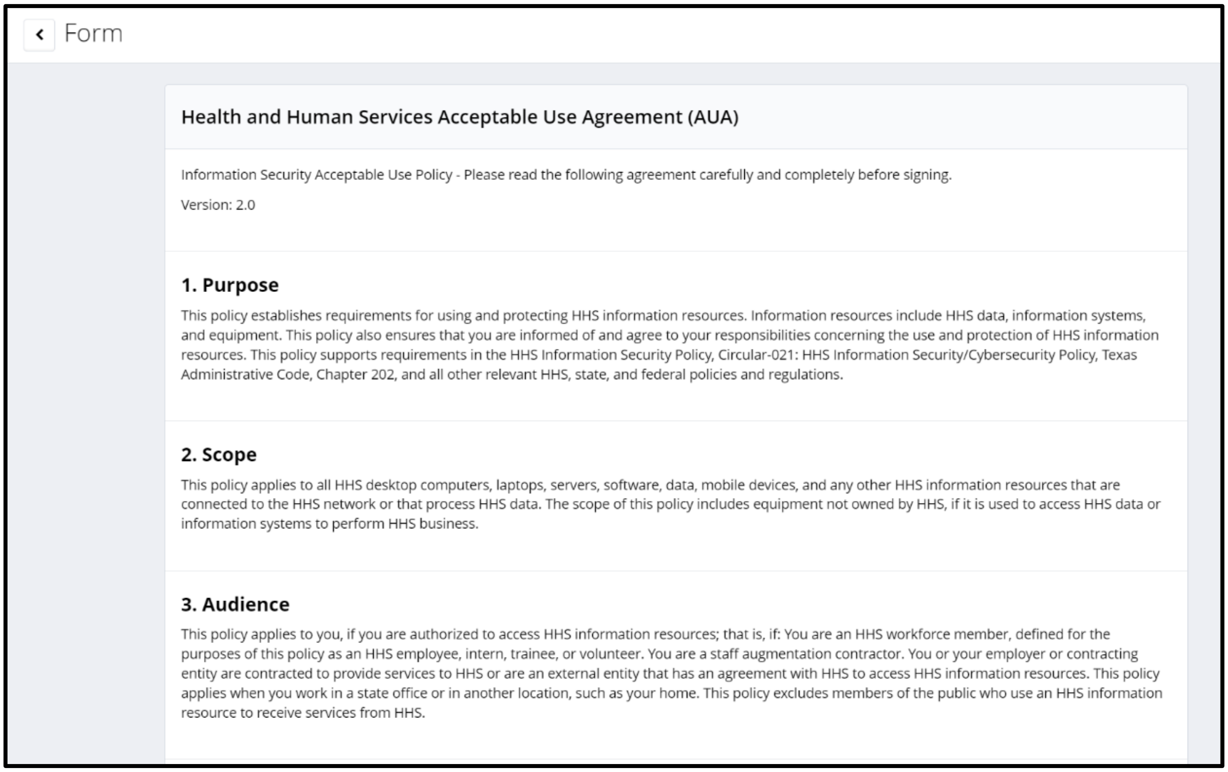
All application access tiles are locked with a lock icon until you complete the Acceptable Use Agreement form (AUA). To review and sign the AUA form, click the **"Acceptable Use Agreement"** tile located on the dashboard.



Review and Sign the AUA Form

The **AUA** tile on the **My Apps** dashboard will take you directly to the AUA form for review and completion.

- You must sign this form once a year, every year.
- The automated HHS system will send email reminders in the following frequency to remind you to complete the form:
  - A first warning is provided fifteen (15) days before AUA form expires;
  - A second warning is provided ten (10) days before AUA form expires;
  - A third warning is provided five (5) days before AUA form expires;
  - A fourth warning is provided each day until the AUA form has reached the expiration date; and
  - A fifth and final warning is provided on the expiration date, 365 days following its last review and signature.
- If you forget to sign the form, all application access will be locked until the form is reviewed and signed.
- Once the form is signed, the system will unlock and renew your application access.



Health and Human Services Acceptable Use Agreement (AUA)

Information Security Acceptable Use Policy - Please read the following agreement carefully and completely before signing.

Version: 2.0

1. Purpose

This policy establishes requirements for using and protecting HHS information resources. Information resources include HHS data, information systems, and equipment. This policy also ensures that you are informed of and agree to your responsibilities concerning the use and protection of HHS information resources. This policy supports requirements in the HHS Information Security Policy, Circular-021: HHS Information Security/Cybersecurity Policy, Texas Administrative Code, Chapter 202, and all other relevant HHS, state, and federal policies and regulations.

2. Scope

This policy applies to all HHS desktop computers, laptops, servers, software, data, mobile devices, and any other HHS information resources that are connected to the HHS network or that process HHS data. The scope of this policy includes equipment not owned by HHS, if it is used to access HHS data or information systems to perform HHS business.

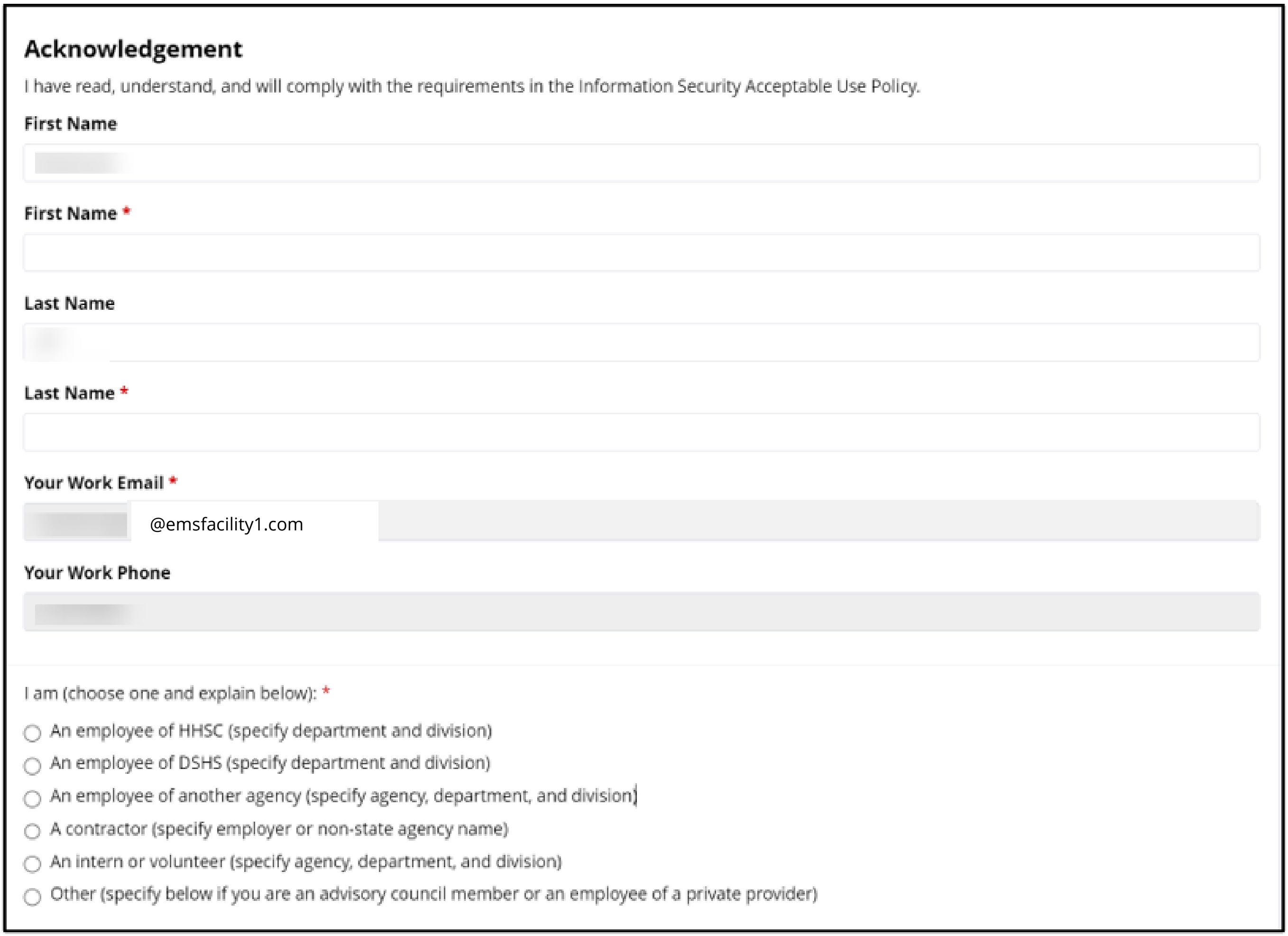
3. Audience

This policy applies to you, if you are authorized to access HHS information resources; that is, if: You are an HHS workforce member, defined for the purposes of this policy as an HHS employee, intern, trainee, or volunteer. You are a staff augmentation contractor. You or your employer or contracting entity are contracted to provide services to HHS or are an external entity that has an agreement with HHS to access HHS information resources. This policy applies when you work in a state office or in another location, such as your home. This policy excludes members of the public who use an HHS information resource to receive services from HHS.

AUA Form Acknowledgement

After you carefully read the AUA form, you must acknowledge and sign the agreement.

- Check the box located next to the statement, "**I acknowledge that I read and understood the agreement, and I agree to comply with its terms**."
- Input your **"First Name"** and "**Last Name"** into the respective text boxes located at the bottom of the agreement.
- Select and identify your role as **"An employee of another agency (specify agency, department and division)"**
- Once you carefully read the AUA form and complete all required entry fields, click the **"Submit"** button.



Acknowledgement

I have read, understand, and will comply with the requirements in the Information Security Acceptable Use Policy.

First Name

[redacted]

First Name *

Last Name

[redacted]

Last Name *

Your Work Email *

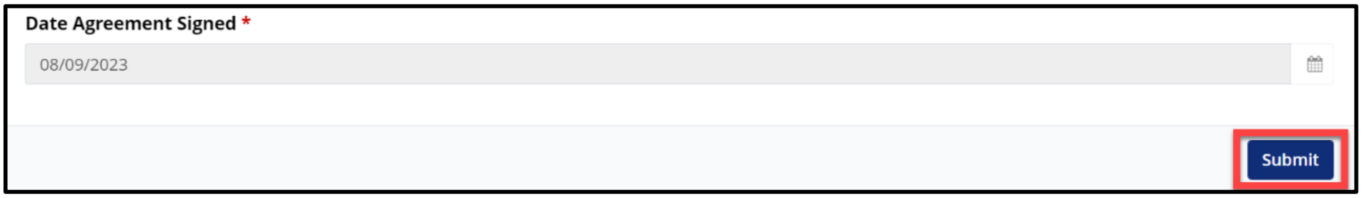
[redacted] @emsfacility1.com

Your Work Phone

[redacted]

I am (choose one and explain below): *

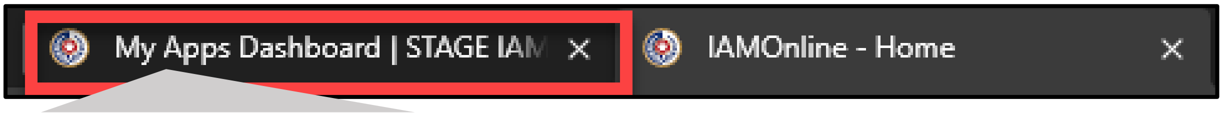
- ○ An employee of HHSC (specify department and division)
- ○ An employee of DSHS (specify department and division)
- ○ An employee of another agency (specify agency, department, and division)
- ○ A contractor (specify employer or non-state agency name)
- ○ An intern or volunteer (specify agency, department, and division)
- ○ Other (specify below if you are an advisory council member or an employee of a private provider)

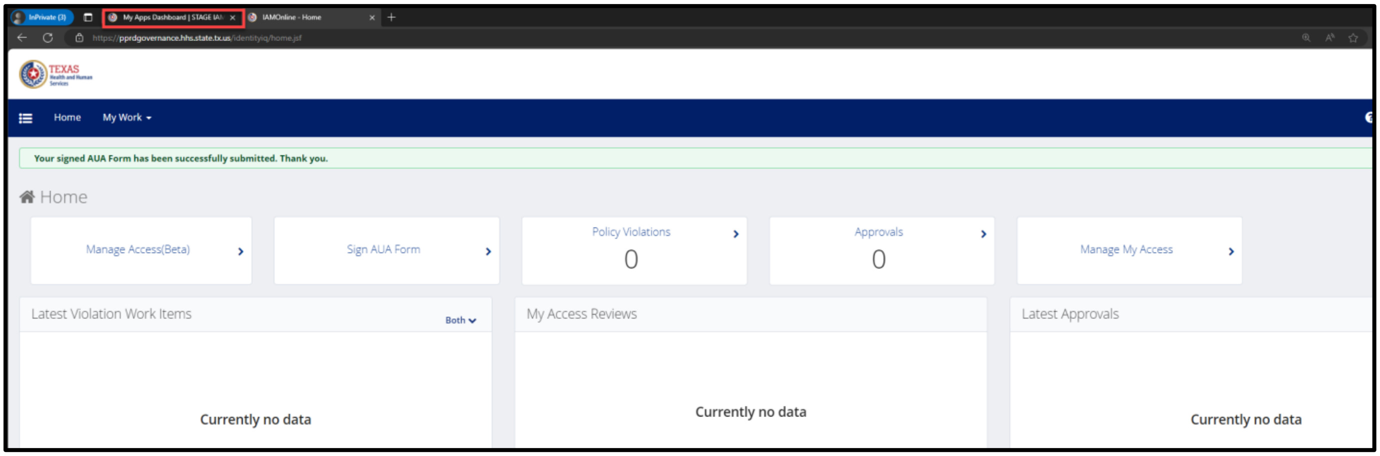


Date Agreement Signed *

08/09/2023

After submitting your AUA form, toggle back to your **MyApps** dashboard webpage.





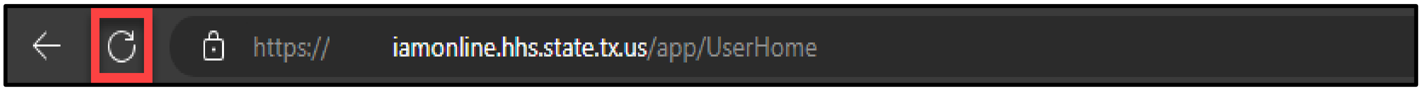
Your signed AUA Form has been successfully submitted. Thank you.

Currently no data

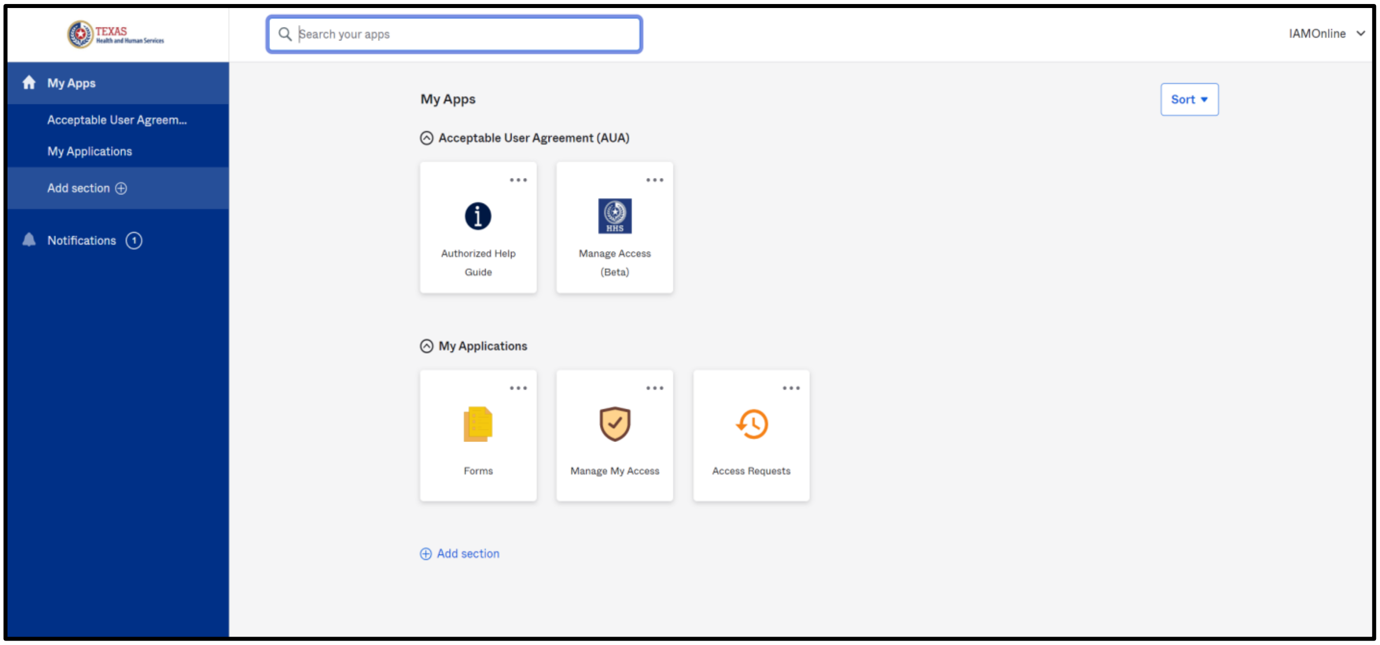
Currently no data

Currently no data

Refresh your browser by clicking the refresh button.

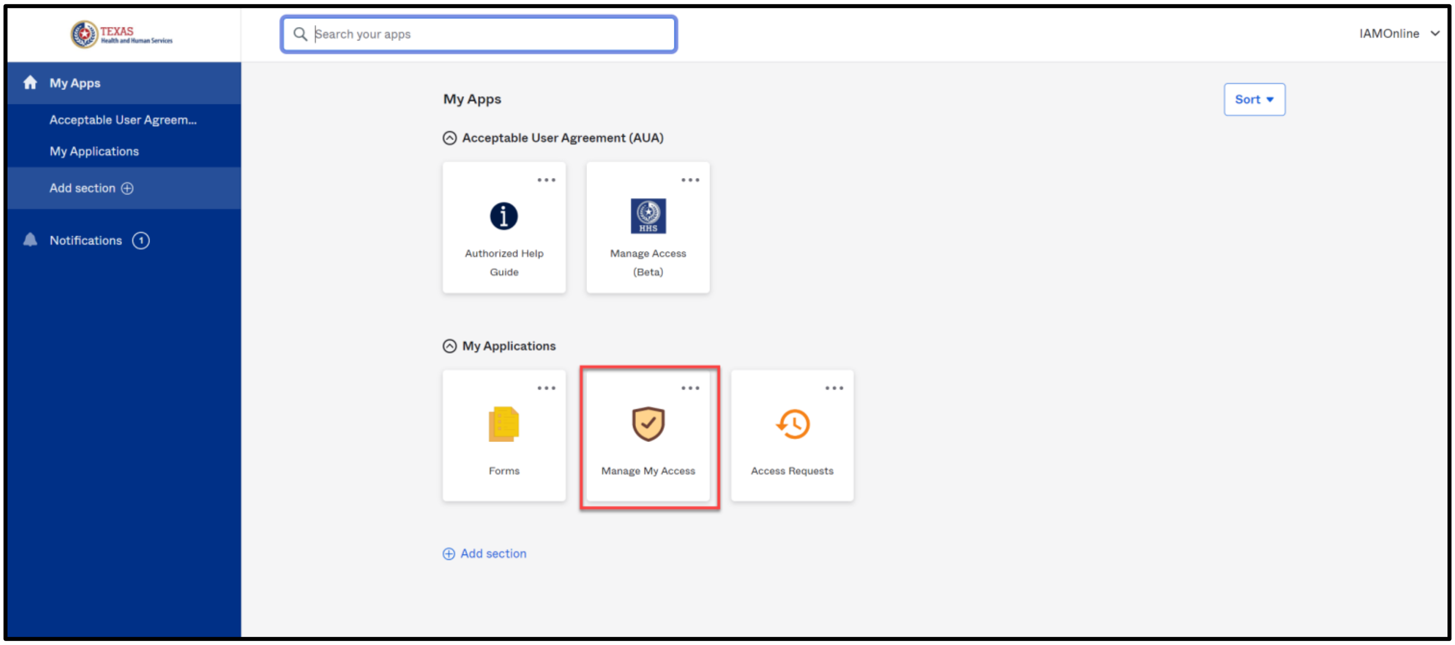


After refreshing your browser, your IAMOnline **MyApps** dashboard tiles will unlock.

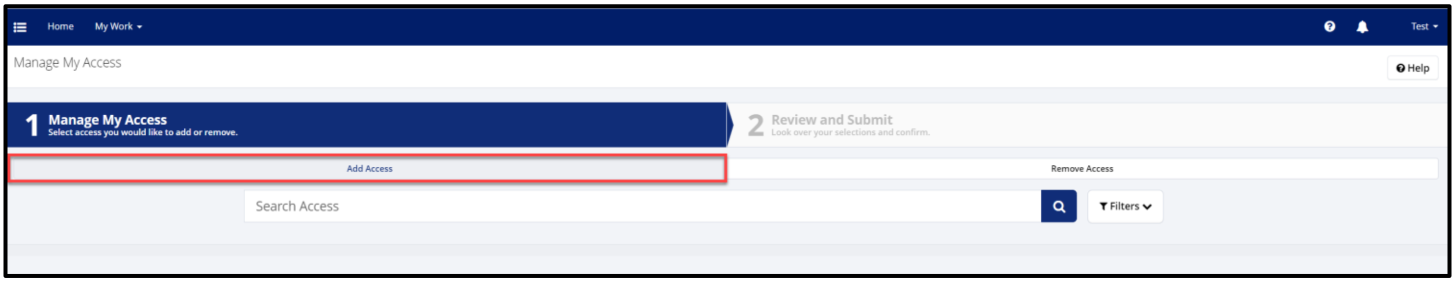


Step 5: Request Access to the EMSTR tile

To request access to EMSTR, select the **"Manage My Access"** tile.

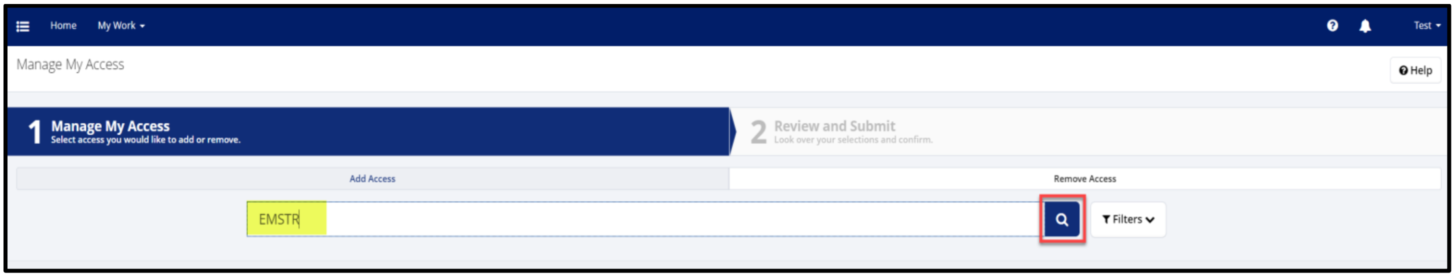


- Click the **"Add Access"** tab to add application access.
- The tab will turn a light grey when selected.



Search for EMSTR

Type "**EMSTR**" in the **Search by Keywords** box



EMSTR

Select the **Magnifying Glass Icon** button to search for the application.

Important Note on Role-Based Access

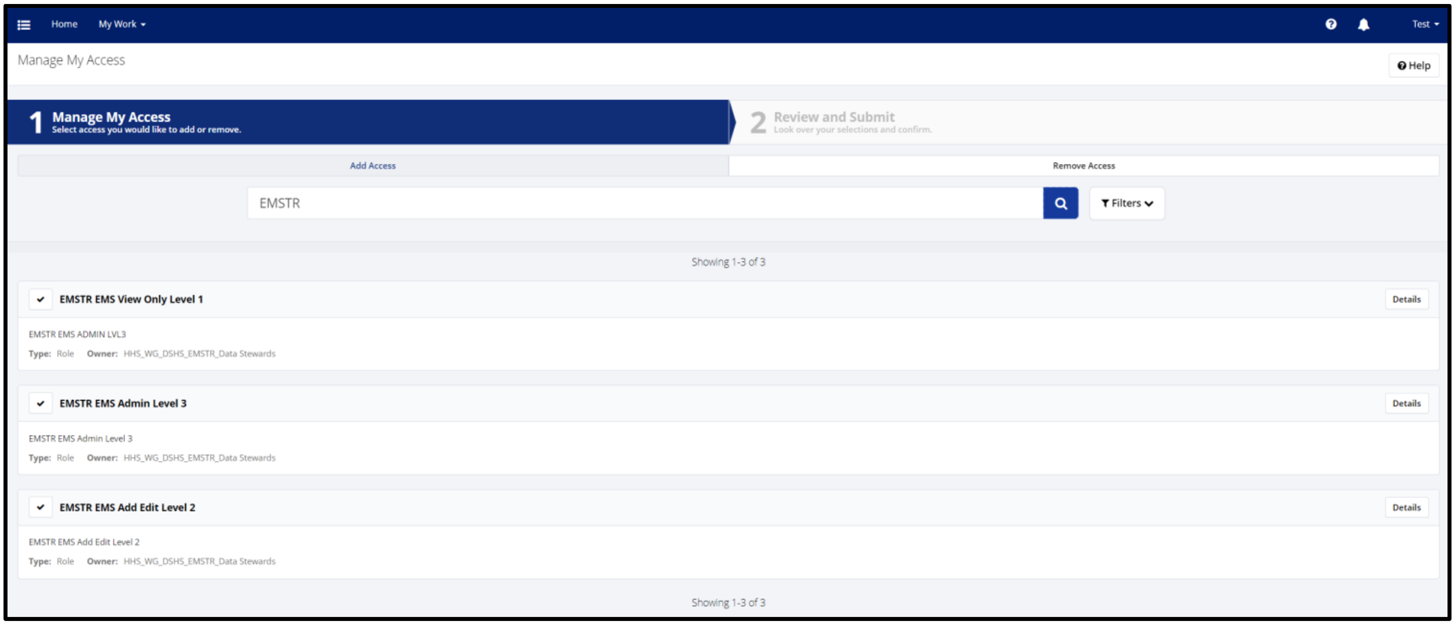
Application access is grouped by role, so you must select the correct EMSTR role access that fits your access needs.

EMSTR has three (3) role types:

- EMSTR View Only Level 1;
- EMSTR Add/Edit Level 2; and
- EMSTR Admin Level 3.

Once you type **"EMSTR"** into the **Search Access** textbox, three types of results will appear: **EMSTR <u>View Only Level 1</u>**, **EMSTR <u>Add/Edit Level 2</u>**, and **EMSTR <u>Admin Level 3</u>.**

- *Example* – ***End-users*** who need limited application access should only request ***EMSTR View Only Level 1*** access.
- *Example* – ***Facility users*** that submit data for their facility but are not facility administrators should select the ***EMSTR Add/Edit Level 2*** access.
- *Example* – ***Organization Administrators*** requesting application access should select the ***EMSTR Admin Level 3*** access.



Manage My Access

1 Manage My Access Select access you would like to add or remove.

2 Review and Submit Look over your selections and confirm.

EMSTR

Showing 1-3 of 3

✓ **EMSTR EMS View Only Level 1**

EMSTR EMS ADMIN LVL3

Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

✓ **EMSTR EMS Admin Level 3**

EMSTR EMS Admin Level 3

Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

✓ **EMSTR EMS Add Edit Level 2**

EMSTR EMS Add Edit Level 2

Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

Showing 1-3 of 3

Select the Correct User Role

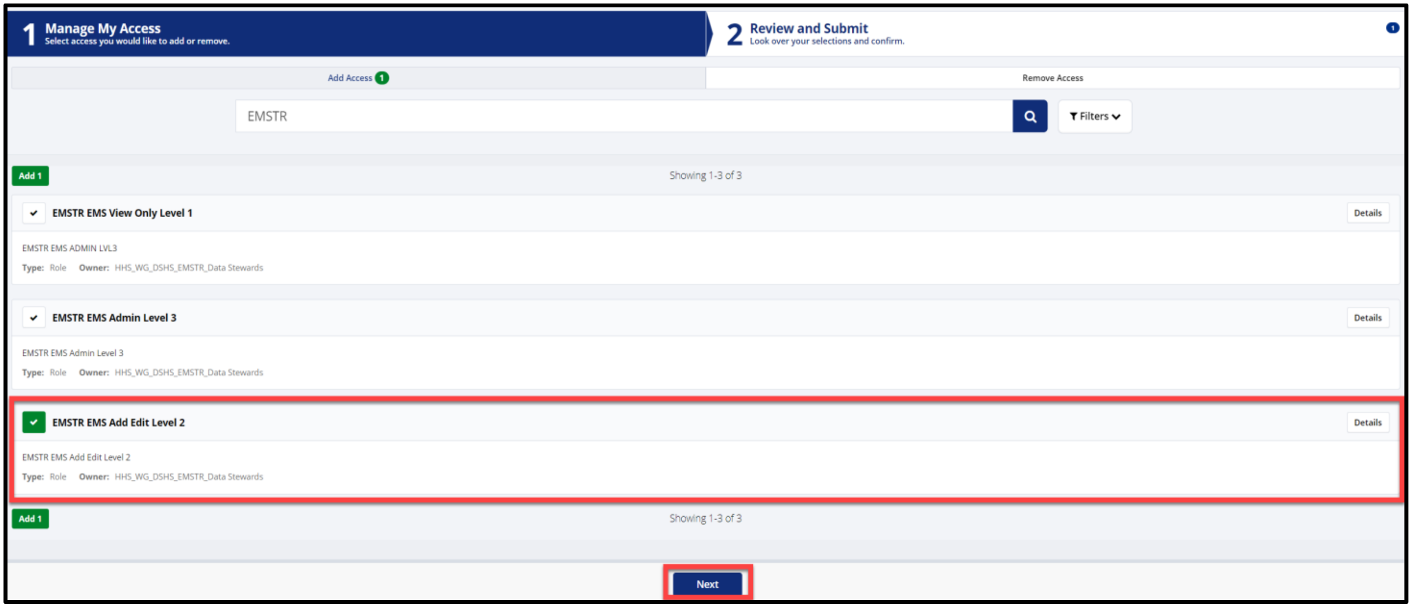
Once you select the M**agnifying Glass Icon** button:

- Click the **Check Mark Icon** to select the EMSTR role type you are requesting.

- The **Check Mark Icon** will turn green once selected.

- Once you select the appropriate EMSTR role level, select the "**Next**" button.

EMS facility providers view example.:



1 Manage My Access
Select access you would like to add or remove.

2 Review and Submit
Look over your selections and confirm.

Add Access 1 | Remove Access

EMSTR

Filters

Add 1 Showing 1-3 of 3

✓ EMSTR EMS View Only Level 1 Details
EMSTR EMS ADMIN LVL3
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

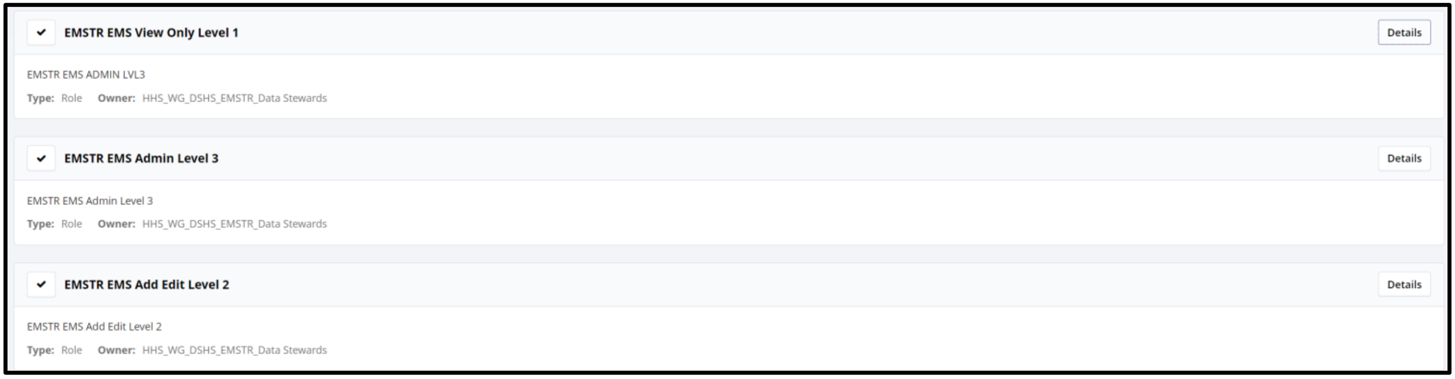
✓ EMSTR EMS Admin Level 3 Details
EMSTR EMS Admin Level 3
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

✓ EMSTR EMS Add Edit Level 2 Details
EMSTR EMS Add Edit Level 2
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

Add 1 Showing 1-3 of 3

Next

Enlarged picture of the role types:



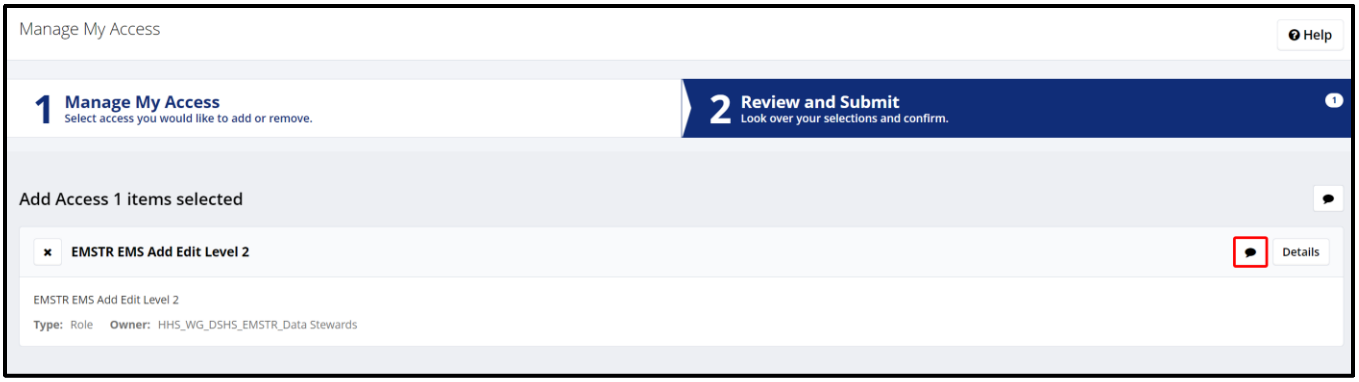
✓ **EMSTR EMS View Only Level 1** Details
EMSTR EMS ADMIN LVL3
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

✓ **EMSTR EMS Admin Level 3** Details
EMSTR EMS Admin Level 3
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

✓ **EMSTR EMS Add Edit Level 2** Details
EMSTR EMS Add Edit Level 2
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

Review and Submit the Request

Once you select the application role type you are requesting, the HHS system will direct you to the **Review and Submit** page.



Manage My Access

1 Manage My Access
Select access you would like to add or remove.

2 Review and Submit
Look over your selections and confirm.

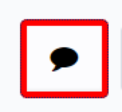
Add Access 1 items selected

EMSTR EMS Add Edit Level 2

EMSTR EMS Add Edit Level 2

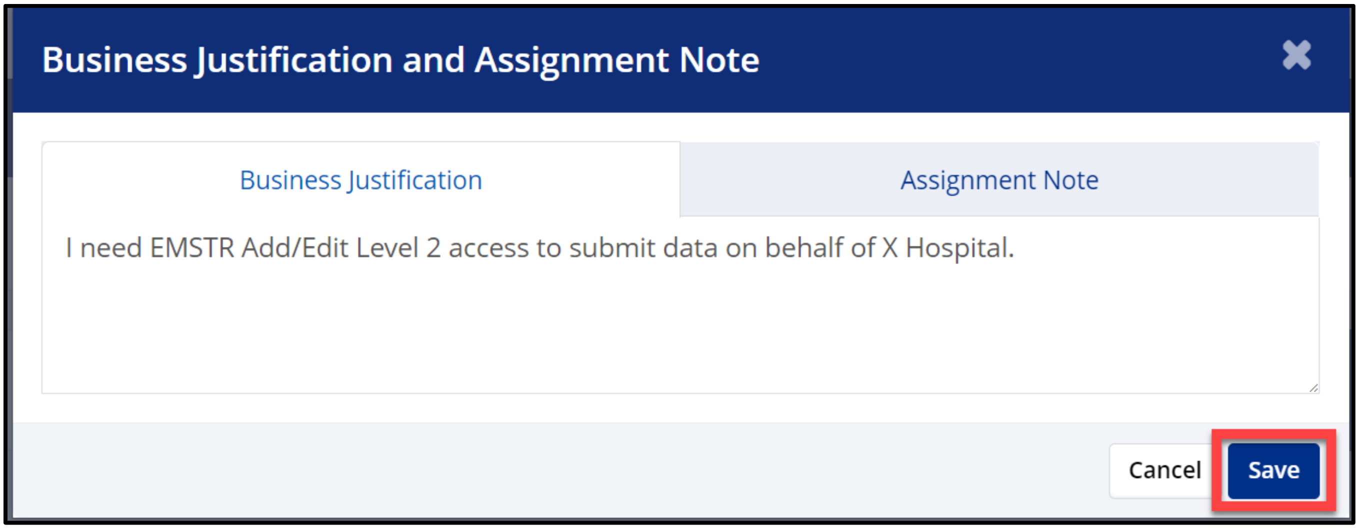
Type: Role **Owner:** HHS_WG_DSHS_EMSTR_Data Stewards

- For a business justification, you are required to leave a comment.
- To leave a comment, select the **Comment Bubble**.



- Leave a comment to explain why you are requesting EMSTR access.
- Click the "**Save"** button.

An example comment is shown below.

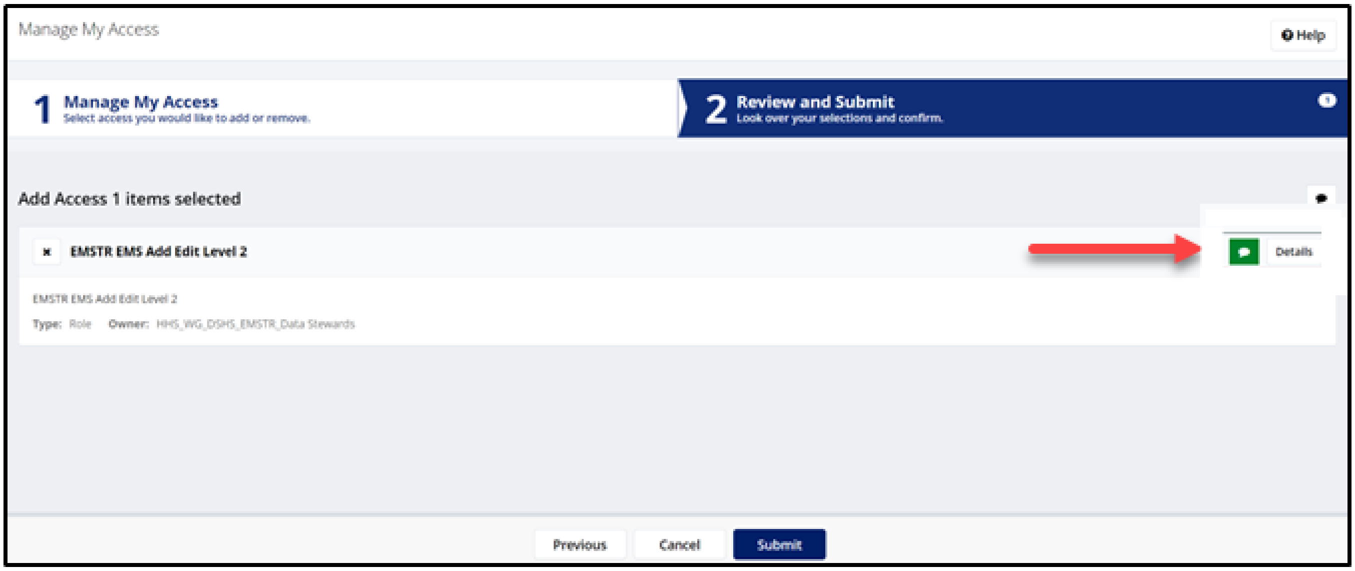


Business Justification and Assignment Note

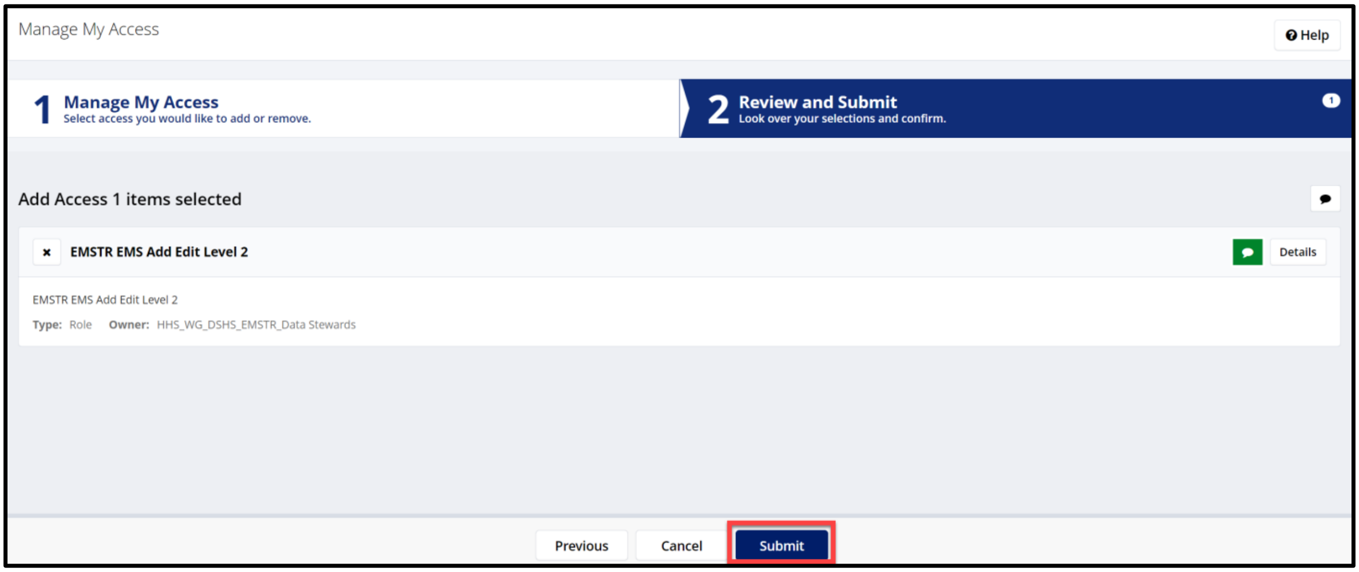
Business Justification | Assignment Note

I need EMSTR Add/Edit Level 2 access to submit data on behalf of X Hospital.

Once you save your comment, the **Comment Bubble Icon** will change from white with a red outline to green.


Manage My Access
Help
1 Manage My Access
Select access you would like to add or remove.
2 Review and Submit
Look over your selections and confirm.
Add Access 1 items selected
EMSTR EMS Add Edit Level 2
Details
EMSTR EMS Add Edit Level 2
Type: Role Owner: HHS_WG_DSHS_EMSTR_Data Stewards
Previous
Cancel
Submit

After reviewing your request, select the **"Submit"** button.


Manage My Access
Help
1 Manage My Access
Select access you would like to add or remove.
2 Review and Submit
Look over your selections and confirm.
Add Access 1 items selected
EMSTR EMS Add Edit Level 2
Details
EMSTR EMS Add Edit Level 2
Type: Role Owner: HHS_WG_DSHS_EMSTR_Data Stewards
Previous
Cancel
Submit

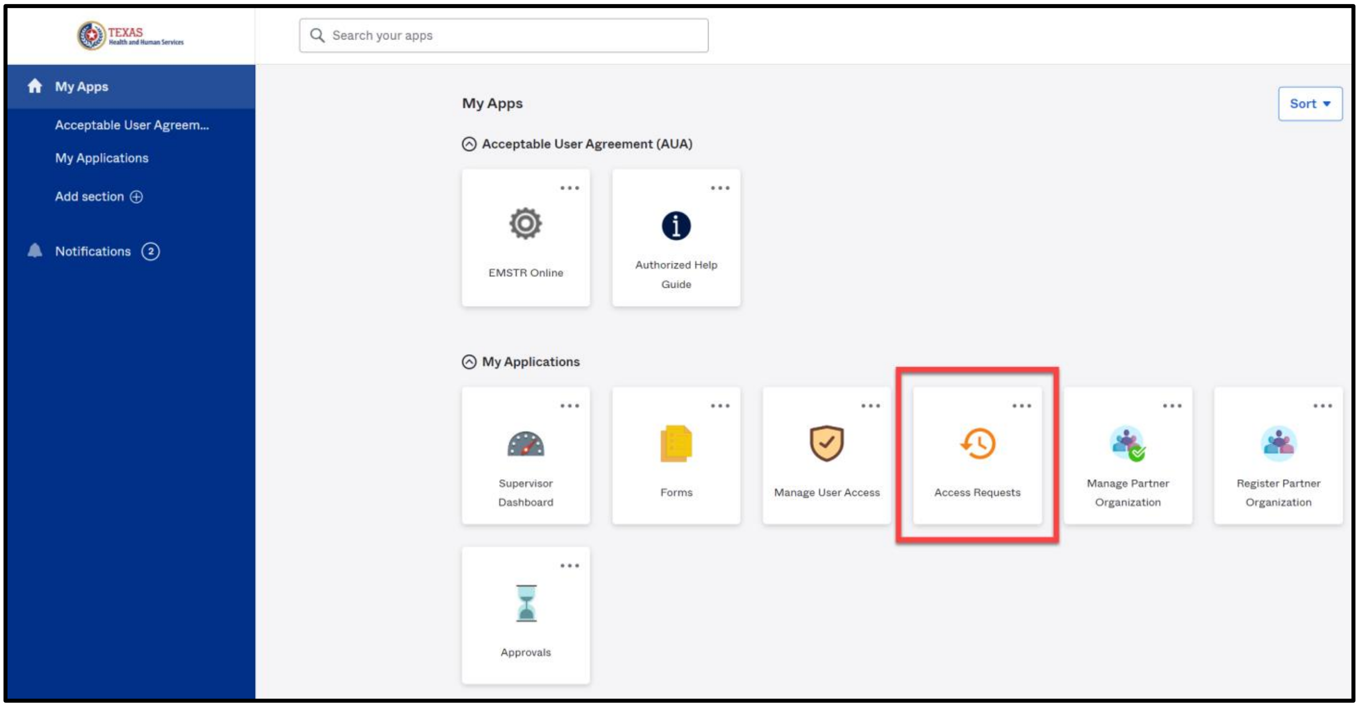
Request Overview

Once you submit your EMSTR application access request, your request will go through an approval process. If you are requesting **EMSTR Add Edit Level 2** access, your organization administration will review and then the DSHS Injury Prevention Unit EMSTR team will review and approve. If you are designated as your organization's administrator or requesting **EMSTR Admin Level 3** access, your request will be sent directly to the Injury Prevention Unit EMSTR team to approve.

Track your Request

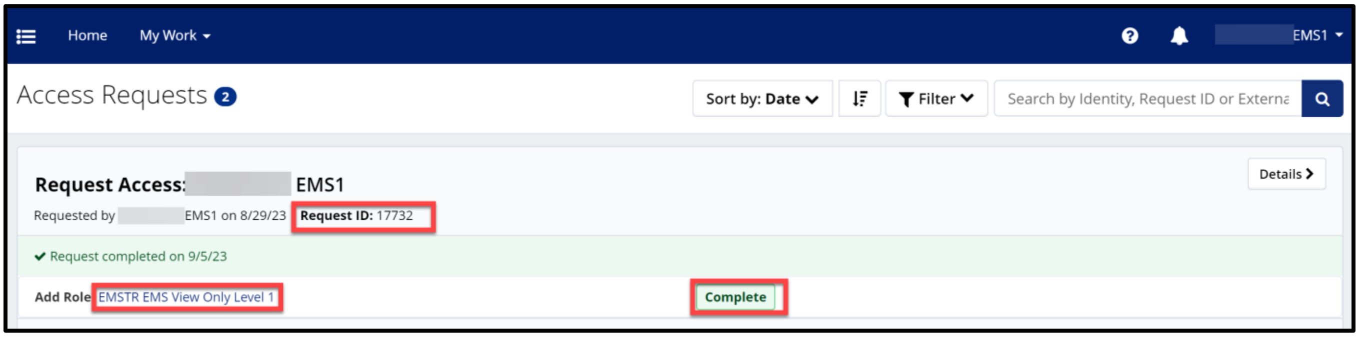
After you submit your request, you can track the status of your access request. The HHS system will send notification emails to EMSTR approvers to approve the request as it moves through the approval process.

- Navigate to the **MyApps** dashboard within IAMOnline.
- Select the "**Access Requests"** tile.



Access Requests

View your access requests and details.



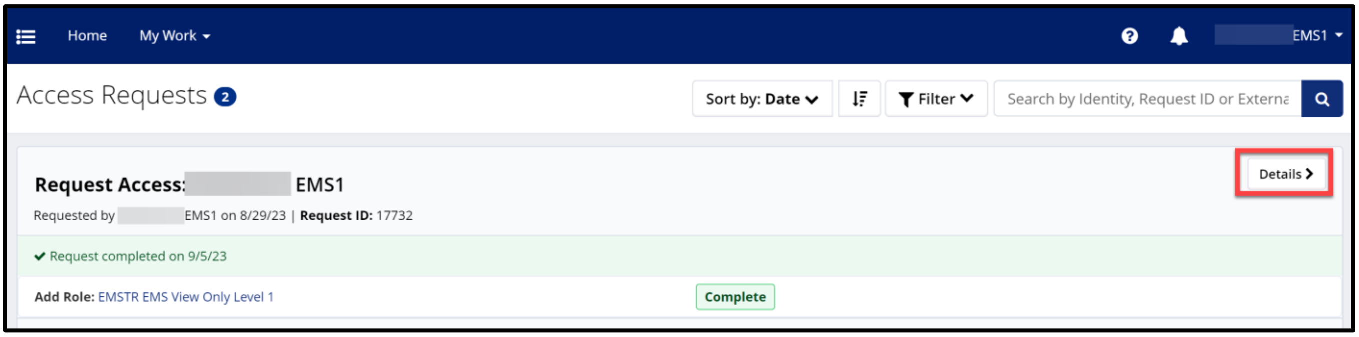
Request Access: [redacted] EMS1

Requested by [redacted] EMS1 on 8/29/23 | **Request ID:** 17732

✓ Request completed on 9/5/23

Add Role: EMSTR EMS View Only Level 1 **Complete**

To view additional details, select the "**Details**" button.



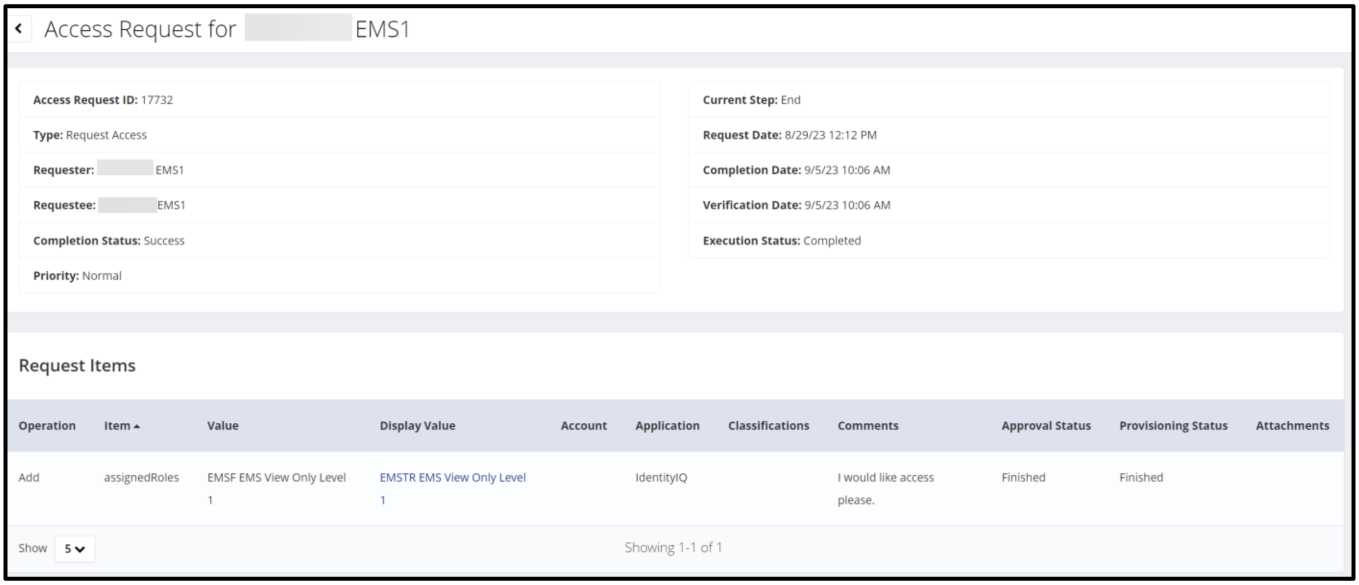
Request Access: [redacted] EMS1

Requested by [redacted] EMS1 on 8/29/23 | **Request ID:** 17732

✓ Request completed on 9/5/23

Add Role: EMSTR EMS View Only Level 1 **Complete**

Once you select the **Details** button, the HHS system will take you to the **Access Request Details** page.


Access Request for [redacted] EMS1

Access Request ID: 17732
Type: Request Access
Requester: [redacted] EMS1
Requestee: [redacted] EMS1
Completion Status: Success
Priority: Normal

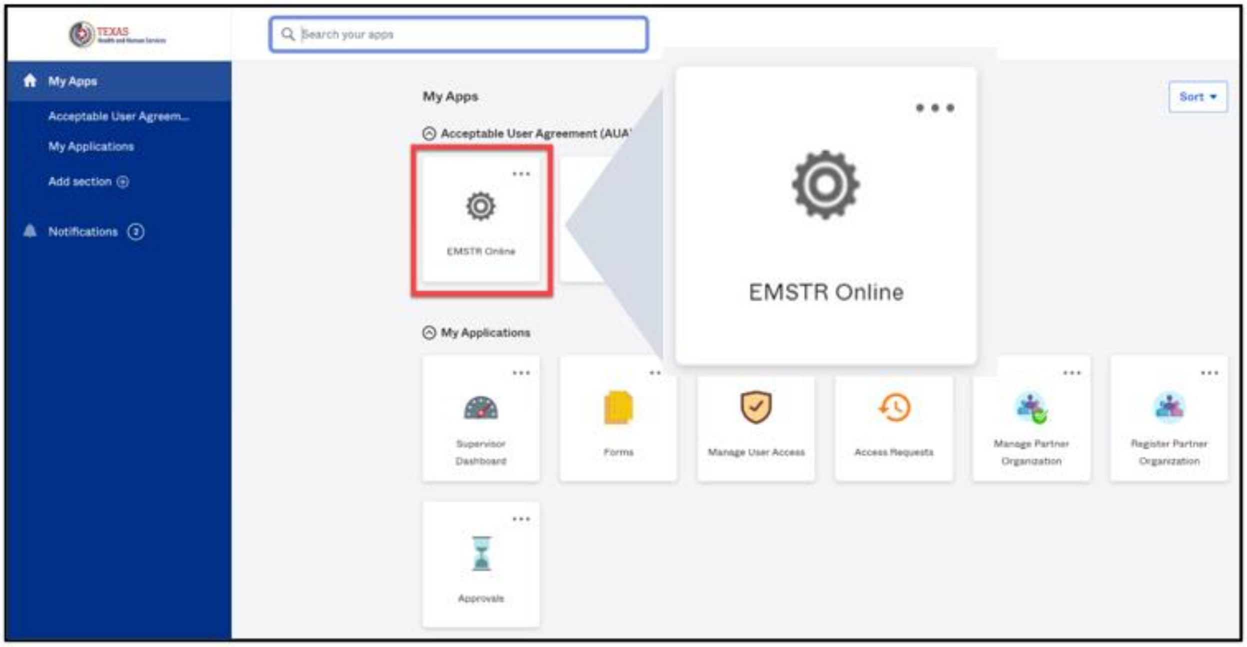
Current Step: End
Request Date: 8/29/23 12:12 PM
Completion Date: 9/5/23 10:06 AM
Verification Date: 9/5/23 10:06 AM
Execution Status: Completed

Request Items

Operation	Item ▴	Value	Display Value	Account	Application	Classifications	Comments	Approval Status	Provisioning Status	Attachments
Add	assignedRoles	EMSF EMS View Only Level 1	EMSTR EMS View Only Level 1		IdentityIQ		I would like access please.	Finished	Finished	

Step 6: Accessing EMSTR

- The system will redirect you to the IAMOnline **My Apps** dashboard.
- Select the **“EMSTR Online”** tile to access the application.



Contact Information

If you have specific EMSTR questions, submit them via email to **injury.web@dshs.texas.gov**.

For IAMOnline questions, visit the Texas Department of State Health Services (DSHS) IAMOnline website **here**.

General Informational Page

General Information

The Emergency Medical Services and Trauma Registries (EMSTR) is made up of four registries – the EMS Registry; the acute Traumatic Injury Registry; the Traumatic Brain Injury Registry / Spinal Cord Injury Registry; and the Submersion Registry. EMSTR is a statewide passive surveillance system that collects reportable event data from EMS providers, hospitals, justices of the peace, medical examiners, and rehabilitation facilities. Texas is home to one of the largest EMS registries in the U.S. with more than 4 million records submitted annually.

TEXAS
Health and Human Services

Texas Department of State Health Services

Our Goals

- To ensure a robust registry reporting framework for recording reportable traumas, submersions, traumatic brain injuries, spinal cord injuries, and EMS runs in Texas.
- To reduce the burden of injury to the public resulting from preventable occurrences using trend analysis.
- To provide data as close to real-time as possible for local, state, and national leadership use.

Our Mission

To improve the Texans' health, safety, and well-being through good stewardship of public resources with a focus on core public health functions.

Contact Information

Emergency Medical Services and Trauma Registries
Texas Department of State Health Services
1100 West 49th Street
Mail Code 1922
Austin, Texas 78756

For program inquiries:
injury.web@dshs.texas.gov

dshs.texas.gov/injury-prevention/ems-trauma-registries

Emergency Medical Services and Trauma Registries

dshs.texas.gov/injury-prevention/ems-trauma-registries/