

EMERGENCY MEDICAL SERVICES AND TRAUMA REGISTRIES

IAMONLINE ACCOUNT ACTIVATION AND LOGIN JOB AID



TEXAS
Health and Human
Services

Texas Department of State
Health Services

Emergency Medical Services and Trauma Registries (EMSTR)

Job Aid for:

All EMSTR Users

Contents

Overview:.....	3
Step 1: Activate Account.....	3
Step 2: Set up security methods	4
Step 3: Access the MyApps Dashboard	10
Step 4: Accessing EMSTR	13
Contact Information	13
General Informational Page.....	14

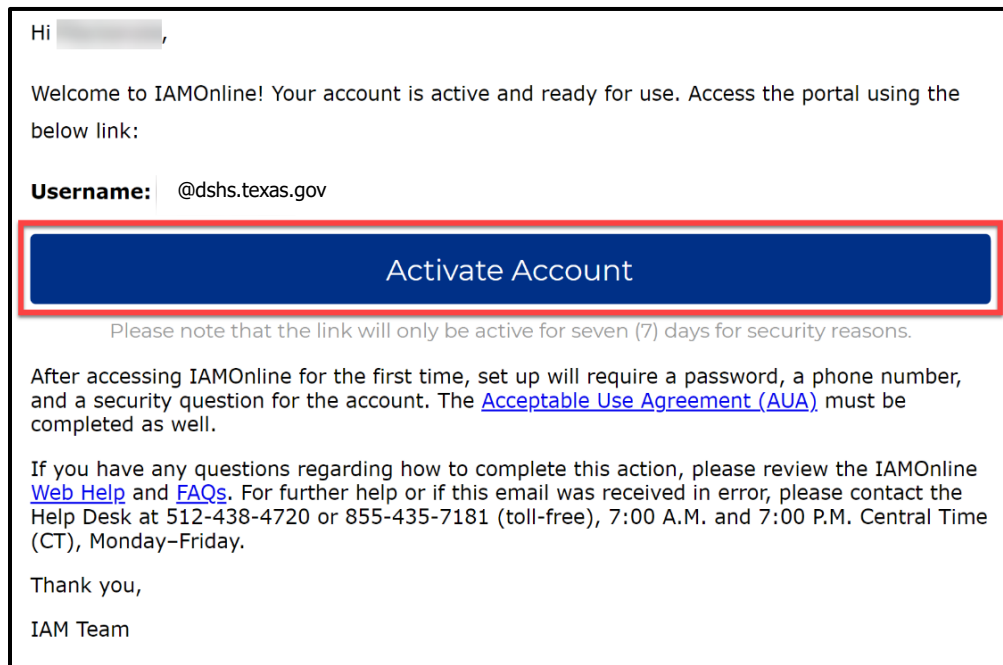
Overview:

This Information and Access Online (IAMOnline) account activation and login job aid provides users with step-by-step instructions on how to activate your IAMOnline account, set-up your account, access the MyApps dashboard, and sign into your account. If you already activated your account and only need instructions on how to login, please access the IAMOnline Login In Only on the [EMSTR New Platform Resources](#) website.

Step 1: Activate Account

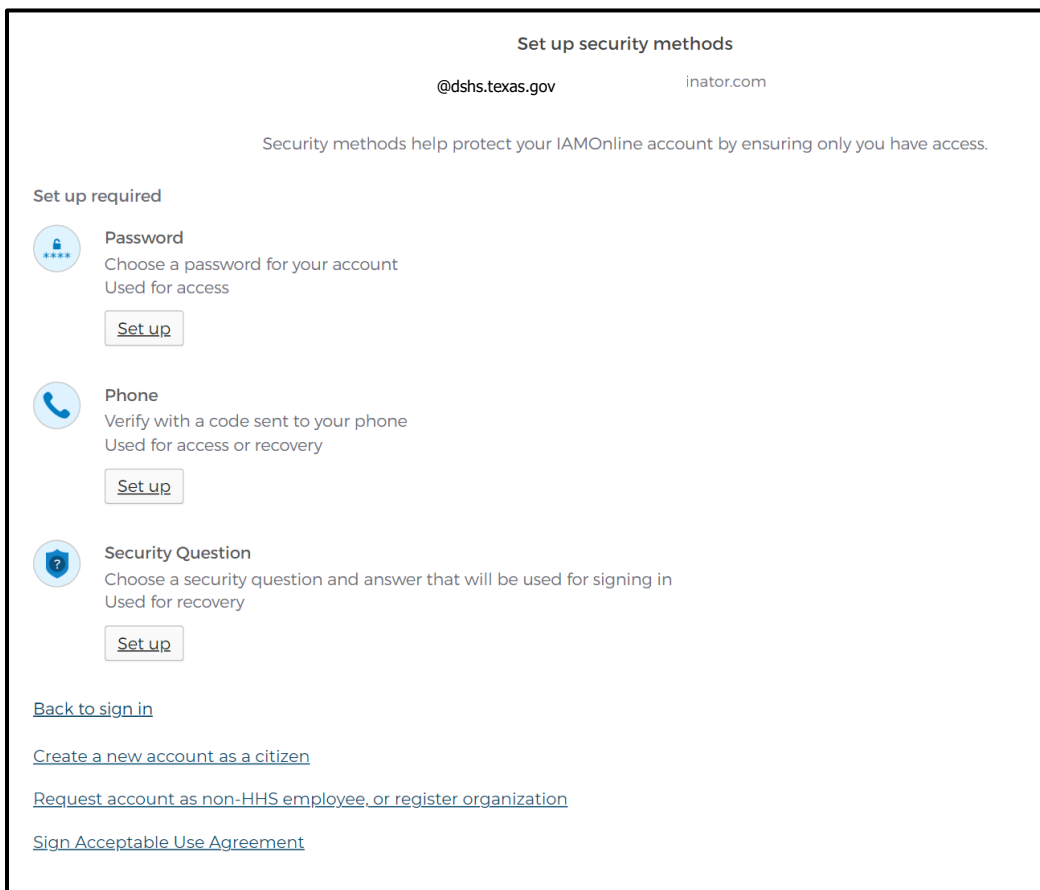
To access your account, find the email from **noreply@okta.com** in your employee email inbox. Check your Junk folder if you don't see it in your inbox. Click the **"Activate Account"** button.

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



Step 2: 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).



The screenshot shows a web page titled "Set up security methods". At the top, it displays the email address "@dshs.texas.gov" and the domain "inator.com". Below this, a message states: "Security methods help protect your IAMOnline account by ensuring only you have access." The page is divided into a section titled "Set up required" which lists three options: "Password", "Phone", and "Security Question". Each option has a corresponding icon (a lock for Password, a phone for Phone, and a question mark for Security Question) and a brief description of its use. Each option also has a "Set up" button. At the bottom of the page, there are four links: "Back to sign in", "Create a new account as a citizen", "Request account as non-HHS employee, or register organization", and "Sign Acceptable Use Agreement".

Set up security methods

@dshs.texas.gov inator.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](#)

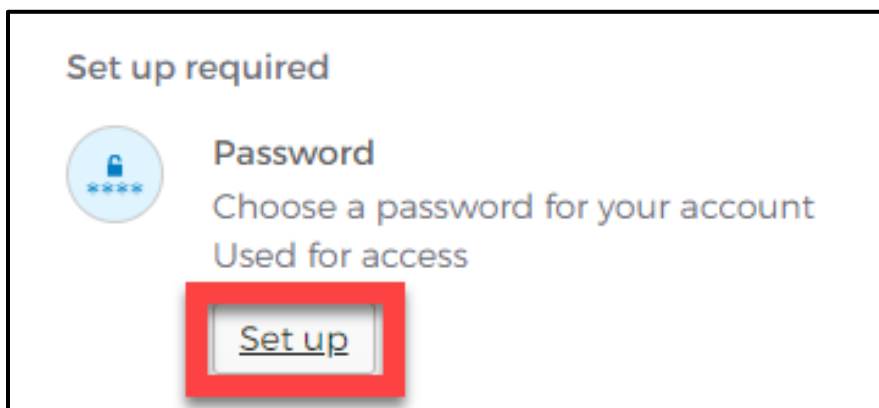
[Create a new account as a citizen](#)

[Request account as non-HHS employee, or register organization](#)

[Sign Acceptable Use Agreement](#)

Password

You need a password to access the account as the system provides a single sign-on to all Texas Health and Human Services (HHS) applications. To set up a **Password**, click the **“Set up”** button.



This is a close-up of the "Password" section from the previous screenshot. It shows the "Set up required" heading, the Password icon (a lock with four asterisks), the text "Password", "Choose a password for your account", and "Used for access". The "Set up" button is highlighted with a red rectangular border.

Set up required

Password
Choose a password for your account
Used for access
[Set up](#)

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.

The screenshot shows a web interface for setting up a password. At the top, there is a blue circular icon with a lock and four asterisks. Below it, the text 'Set up password' and '@dshs.texas.gov' are displayed. A section titled 'Password requirements:' lists the following criteria:

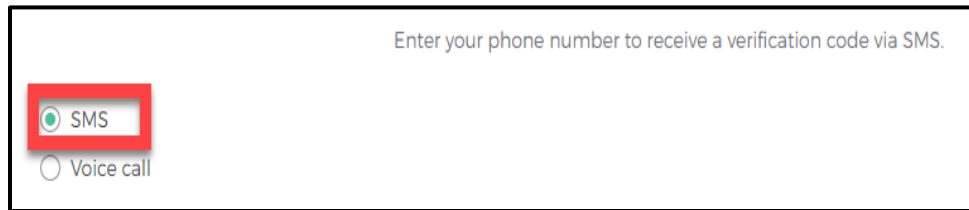
- At least 8 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Does not include your first name
- Does not include your last name
- Your password cannot be any of your last 24 passwords

Below the requirements, there are two text input fields. The first is labeled 'Enter password' and the second is labeled 'Re-enter password'. Both fields are highlighted with red boxes. At the bottom of the form, there is a blue button labeled 'Next', which is also highlighted with a red box.

- 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 **“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.



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

☒ SMS

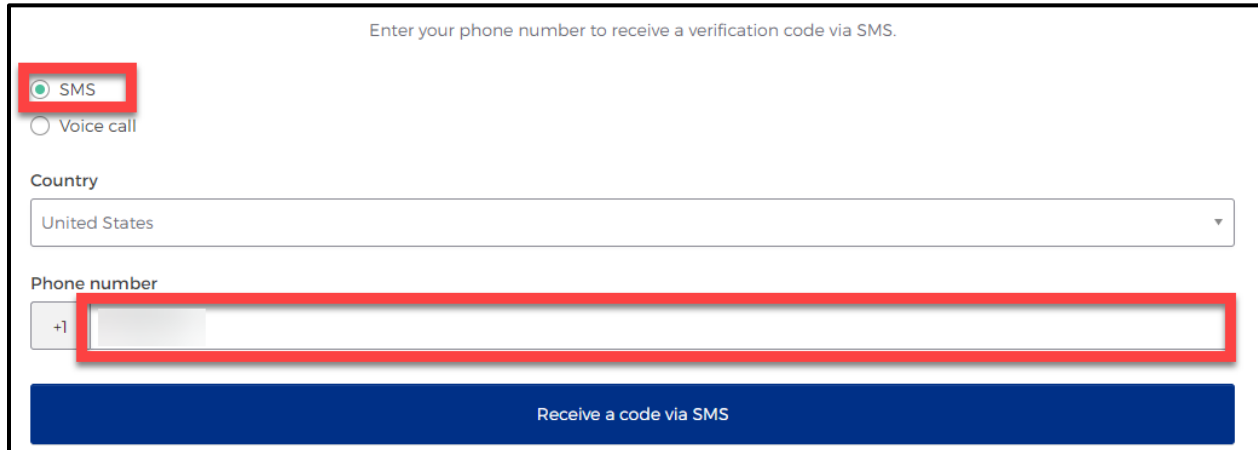
☐ Voice call

Example of SMS option selected.

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

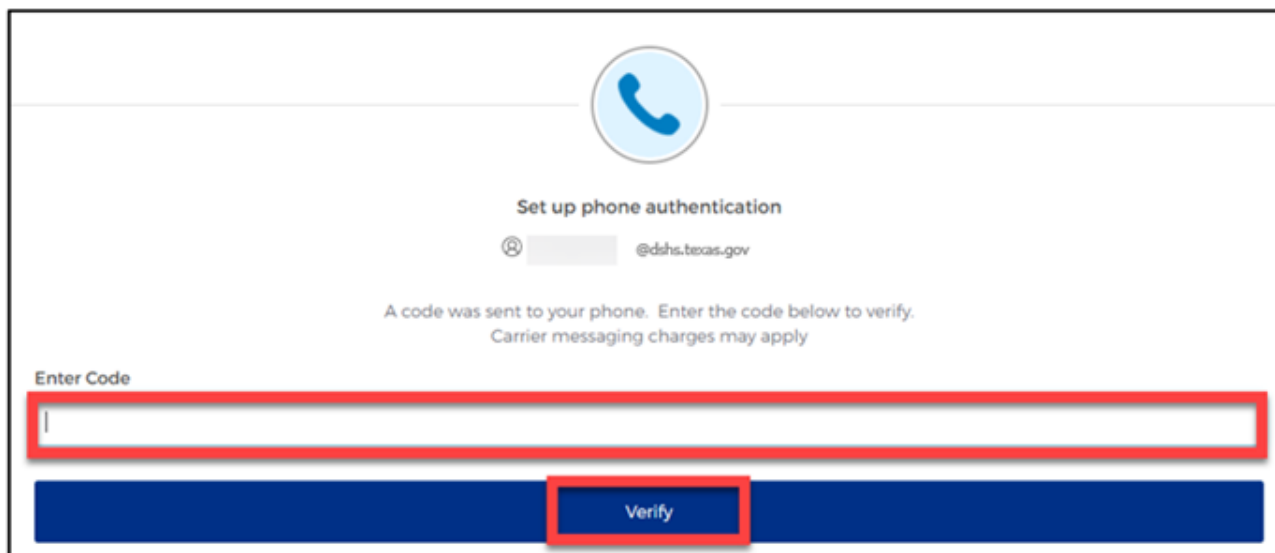
United States

Phone number

+1

Receive a code via SMS

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



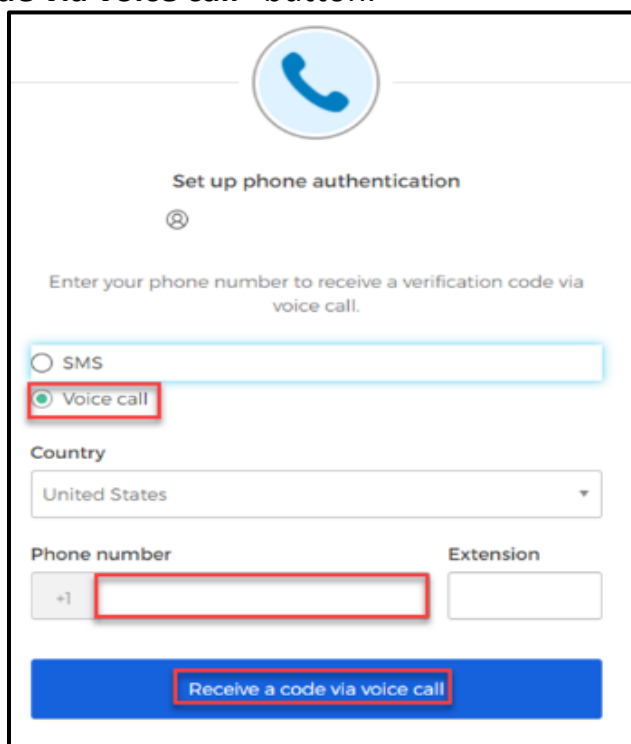
The screenshot shows a web interface for setting up phone authentication. At the top, there is a blue telephone icon in a circle. Below it, the text "Set up phone authentication" is displayed. Underneath, there is a small icon of a person and the text "@dshs.texas.gov". A message states: "A code was sent to your phone. Enter the code below to verify. Carrier messaging charges may apply". Below this message is a text input field labeled "Enter Code" with a red border. At the bottom, there is a blue button labeled "Verify" with a red border.

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

Voice Call

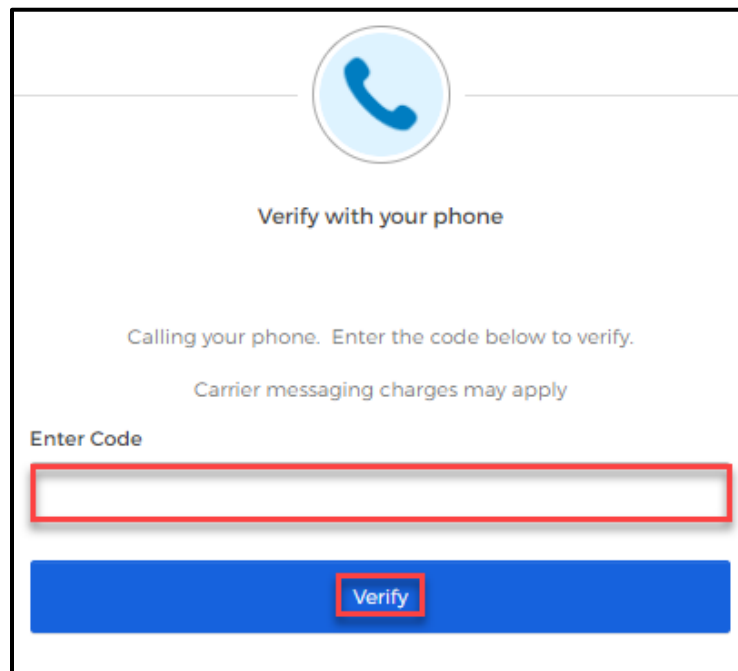
The second option to verify the account is a voice call. The system can provide an automated **verification code** via **Voice call**.

- 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.



The screenshot shows a web interface for setting up phone authentication. At the top, there is a blue telephone icon in a circle. Below it, the text "Set up phone authentication" is displayed. Underneath, there is a small icon of a person. A message states: "Enter your phone number to receive a verification code via voice call." Below this message are two radio button options: "SMS" and "Voice call". The "Voice call" option is selected and has a red border. Below the radio buttons is a "Country" dropdown menu with "United States" selected. Below the country dropdown are two text input fields: "Phone number" and "Extension". The "Phone number" field has a red border and a "+1" prefix. At the bottom, there is a blue button labeled "Receive a code via voice call" with a red border.

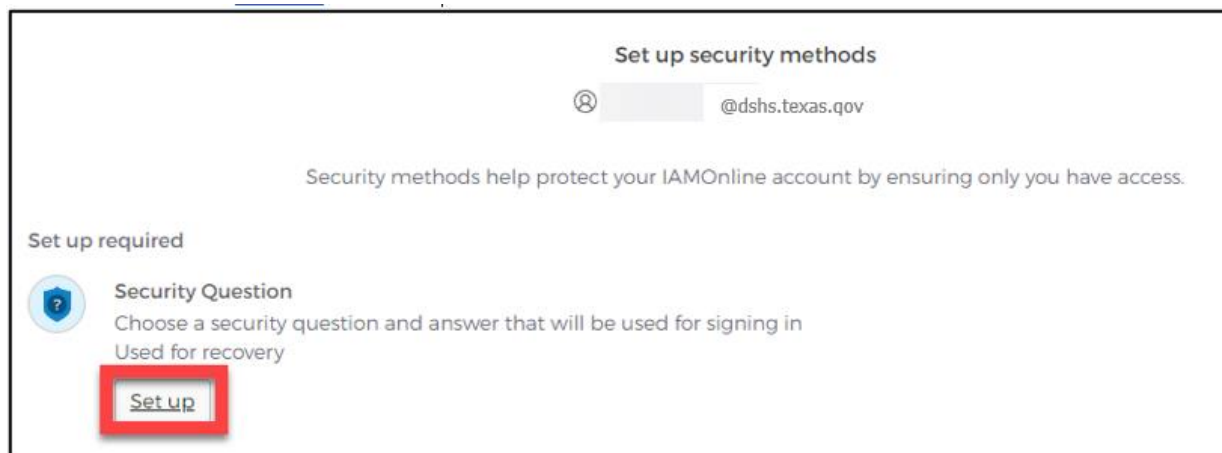
- Type the code provided by the voice call in the **Enter Code** text box and click the **“Verify”** button.



Security Question

Set up a security question to protect the account.

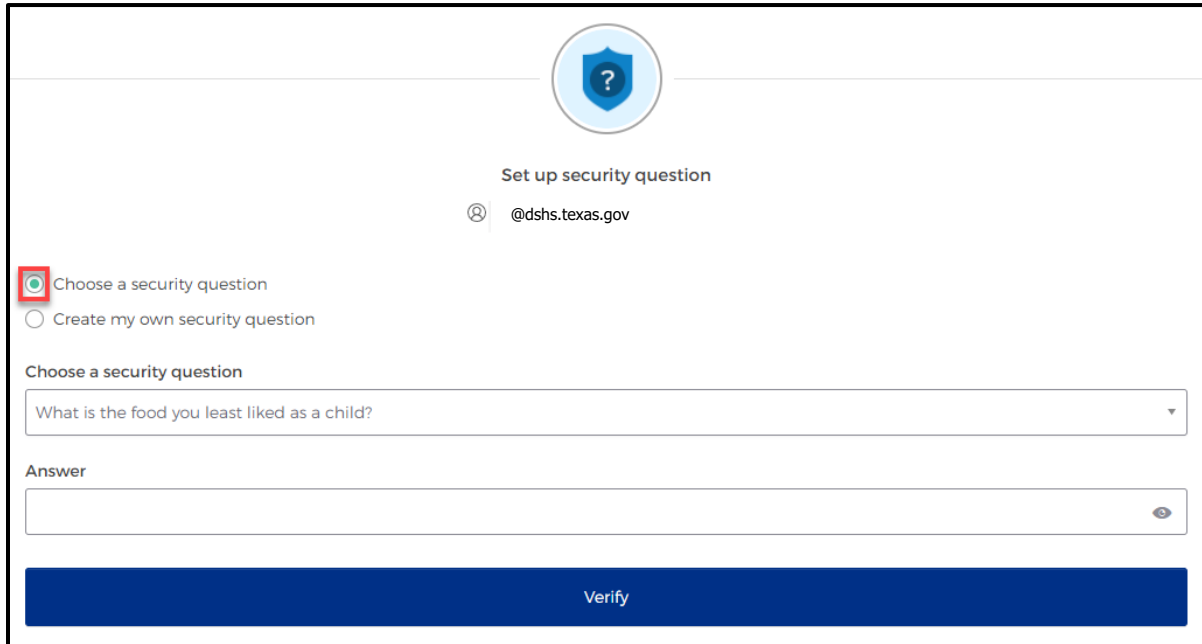
- Click the **“Set up”** button.



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

- To choose a security question, select the **“Choose a security question”** option.
- Select the drop-down icon ▼ and scroll to select a security question.



Set up security question

@dshs.texas.gov

☒ Choose a security question

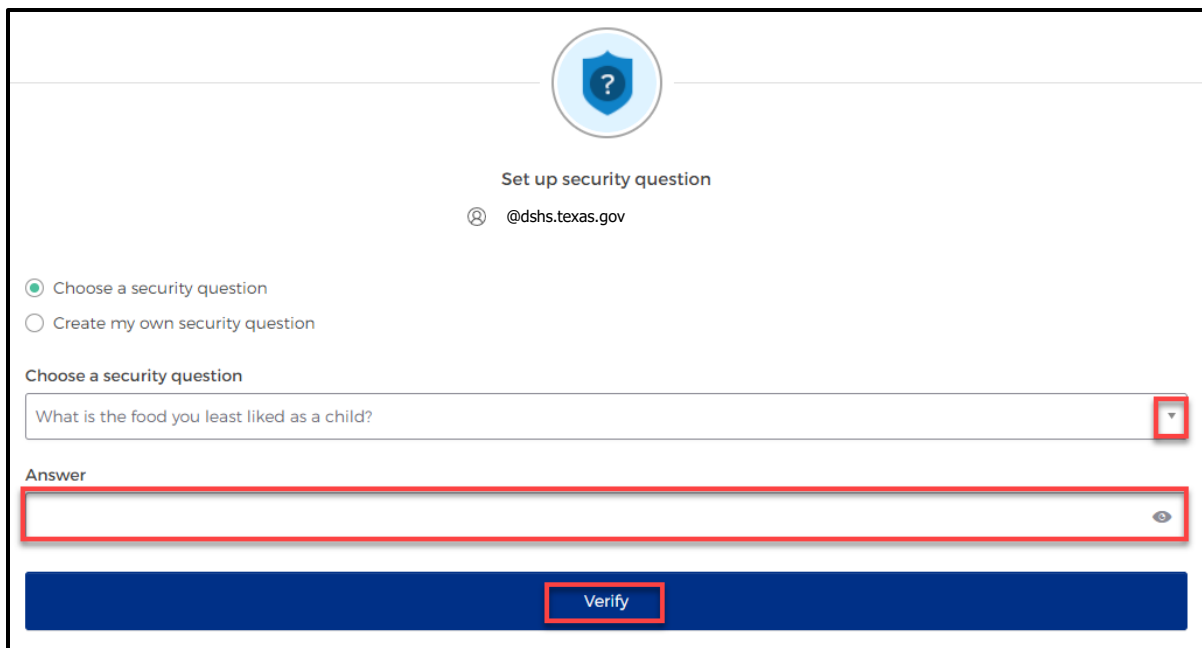
☐ Create my own security question

Choose a security question

What is the food you least liked as a child?

Answer

Verify



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?

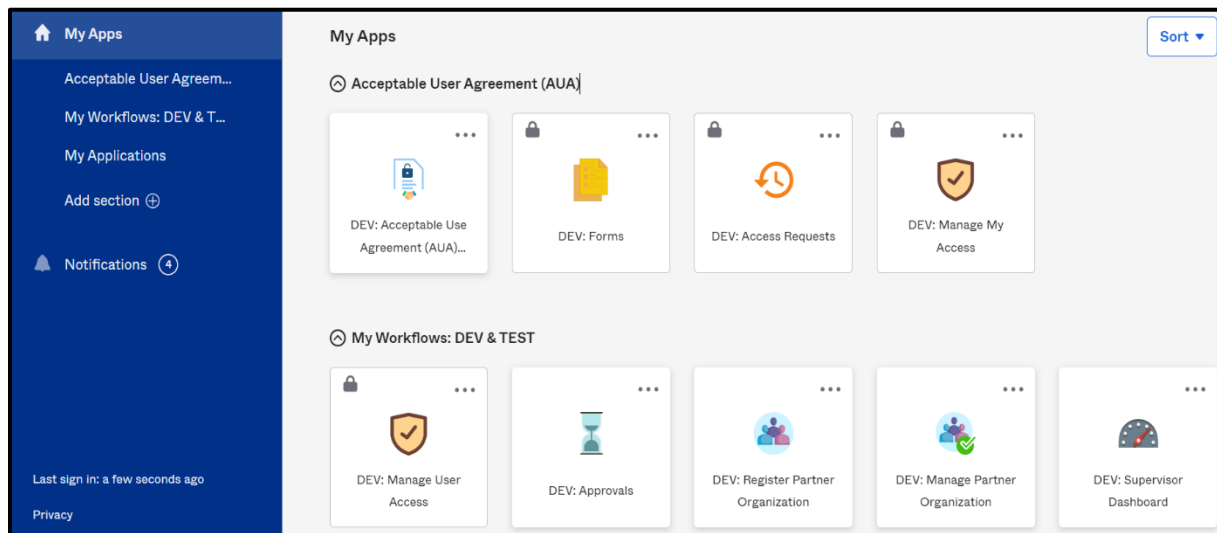
Answer

Verify

Step 3: Access the MyApps Dashboard

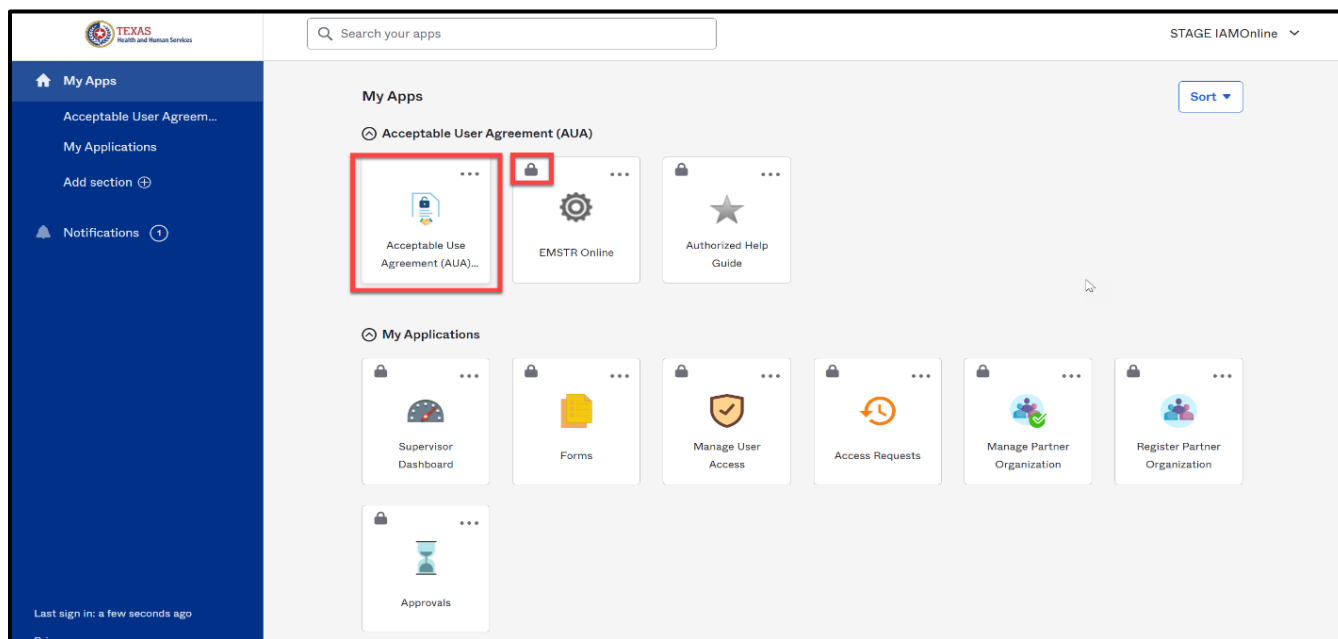
Your account set up is now complete and you can access your **My Apps** dashboard.

- 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.

The screenshot shows a web form titled "Form" with a back arrow icon. The main content area is titled "Health and Human Services Acceptable Use Agreement (AUA)". Below the title, it states "Information Security Acceptable Use Policy - Please read the following agreement carefully and completely before signing." and "Version: 2.0". The form is divided into three sections: "1. Purpose", "2. Scope", and "3. Audience".

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, contractor, or intern with your associated organization.
- 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

First Name *

Last Name

Last Name *

Your Work Email *

Your Work Phone

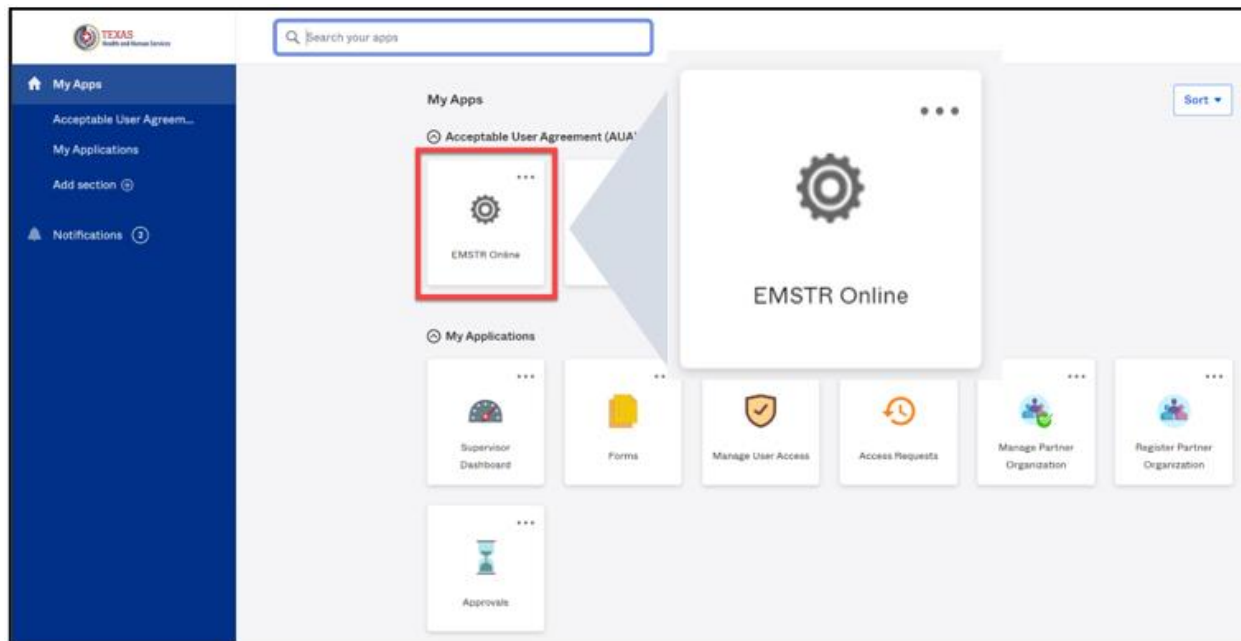
I am (choose one and explain below): *

☐ 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 *

Step 4: 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.



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/](https://dshs.texas.gov/injury-prevention/ems-trauma-registries/)***