

Identify.

Report.

Protect.

Children's Incident Tracking and Reporting User Guide

May 3, 2024

Table of Contents

1 Introduction.....	1
1.1 Purpose of the Children’s Incident Tracking and Reporting Application	1
2 Security Roles	2
2.1 Security Roles	2
3 Logging in for First Time	3
3.1 Reset Password	15
3.2 Unlocking an Account.....	28
4 Accessing Children’s Incidents.....	39
4.1 Search Function.....	49
4.2 Filter for Incidents	49
4.3 Participant Incident History.....	50
4.4 Inactivating an Incident	52
4.5 Agency Participants Dashboard.....	52
4.5.1 Search Function.....	53
5 Creating an Incident for a Participant Enrolled in CLTS.....	55
6 Creating an Incident for an Unlisted Participant	71
7 Legacy Incident Data	72
8 Reports	74
9 Viewing Incident History.....	80
10 Editing an Incident.....	81
11 Appendix A: Security Roles and Allowable Functions.....	82
12 Appendix B: Supported Web Browsers	84
13 Appendix C: Support Resources	86

14 Appendix D: Data Fields and Menu Options.....	87
14.1 Incident Type.....	87
14.2 Incident Type Detail.....	87
14.3 Where did the incident occur?.....	88
14.4 Outcome.....	89
14.5 Remediation Action 1.....	90
14.6 Preventative Strategy 1.....	91
12 Appendix E: Glossary.....	93

1 Introduction

The Children's Long-Term Support (CLTS) Waiver Program and Children's Community Options Program (hereafter referred to collectively as "CLTS programs") are built upon a foundation of primary program values. These values support individual choice; the enhancement of relationships; the building of accessible, flexible service systems; the achievement of optimum physical and mental health for the participant; and the promotion of presence, participation, and optimal social functioning in the community. CLTS program values further seek to ensure that children and families are treated with respect and assure that service systems empower the individual, build on their strengths, enhance individual self-worth, and supply the tools necessary to achieve maximum independence and community participation.

Incident resolution and prevention are essential to promote and support the health, safety, and welfare of children with disabilities. CLTS programs must have policies and systems in place to effectively identify, address, and seek to prevent risk to a child's health and safety with a focus on engaging in active awareness and coordinating the efforts of all people who support the child in their home and community.

1.1 Purpose of the Children's Incident Tracking and Reporting Application

The Children's Incident Tracking and Reporting (CITR) application is a secure data collection, tracking and reporting aid to support local, regional, and state staff to work as a team to identify, track, and report incidents.

- The information collected enables the Wisconsin Department of Health Services (DHS) to identify trends and create new methods that may help prevent risk to children's health and safety at the local and state level.
- The specific focus is to collect and share the information with the appropriate people to engage in active awareness and coordinating the efforts of all people who support the child in their home and community.

2 Security Roles

2.1 Security Roles

Seven different security roles are available through the LTCare Information Exchange System (LTCare IES). Access to certain features or functions on the application is determined by the security role assigned to a user. Through these different security roles, a high level of security and accountability is maintained. A list of security roles and their allowable functions is available in [Appendix A: Security Roles and Allowable Functions](#).

Note: Information about setting up new users, inactivating users and managing permissions is available in the User Management Guide, which can be accessed from the menu on the left side of the LTCare Information Exchange System page. This link will only appear for users who have access to these functions.

Note: Users are recommended to use the Google Chrome or FireFox web browsers. A complete list of computing platforms with web browsers and versions supported is available in [Appendix B: Supported Web Browsers](#). Resources for help desk support are also available in [Appendix C: Support Resources](#).

3 Logging in for First Time

CITR account users will be required to complete the steps for multi-factor authentication (MFA) when logging in for the first time and every 60 days thereafter.

With MFA, users are asked to provide two authentication methods to verify their identity when logging in to the CITR application. MFA will protect accounts against unauthorized access in case user login credentials are compromised.

MFA will be required to log in when a user changes any of the following account information:

- Account password
- Email address

When using MFA, a user will be sent a one-time code through their choice of email, text message (SMS), or phone call.

1. Access the CITR application at <https://ltcareies.forwardhealth.wi.gov/citr>.

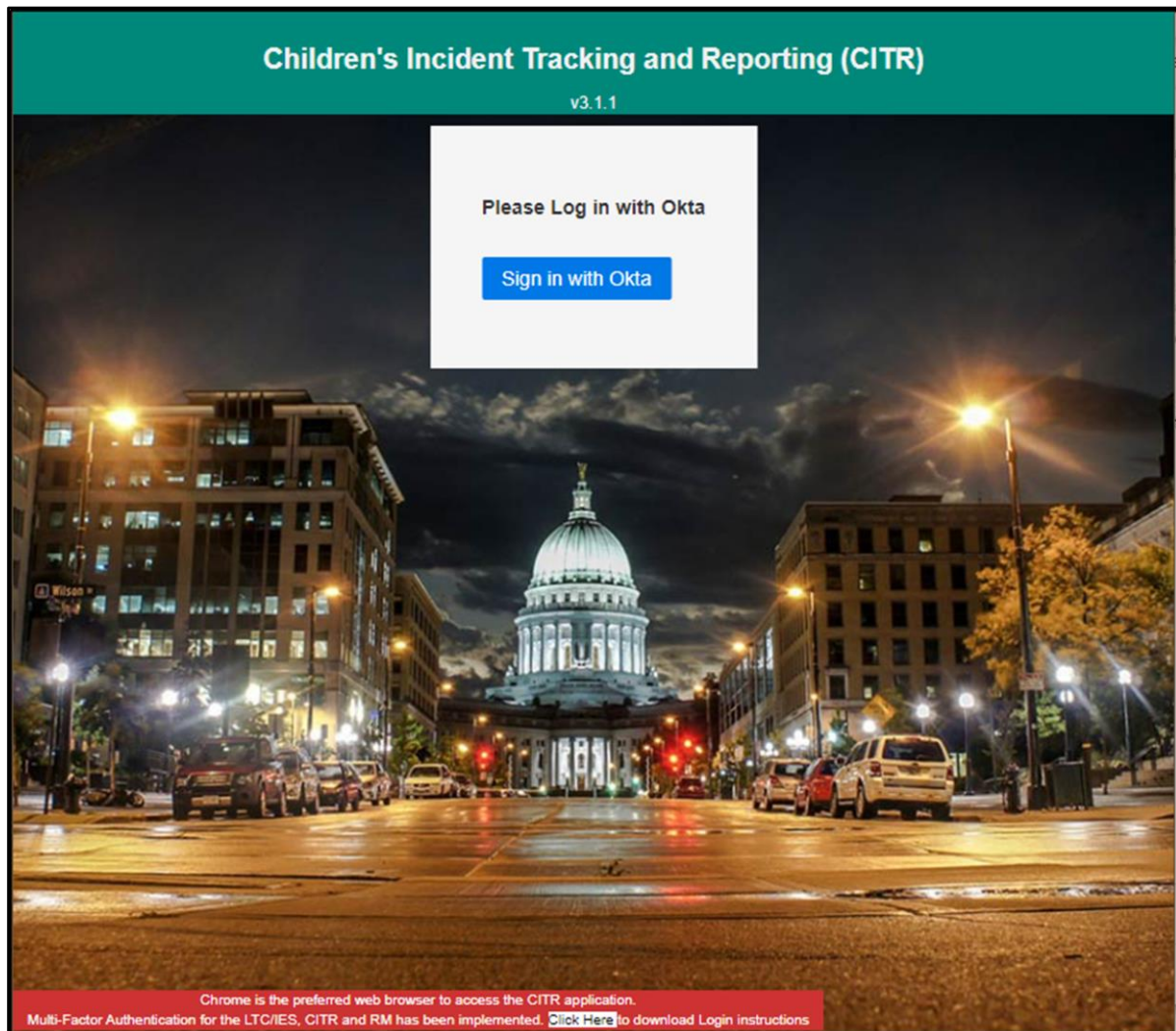
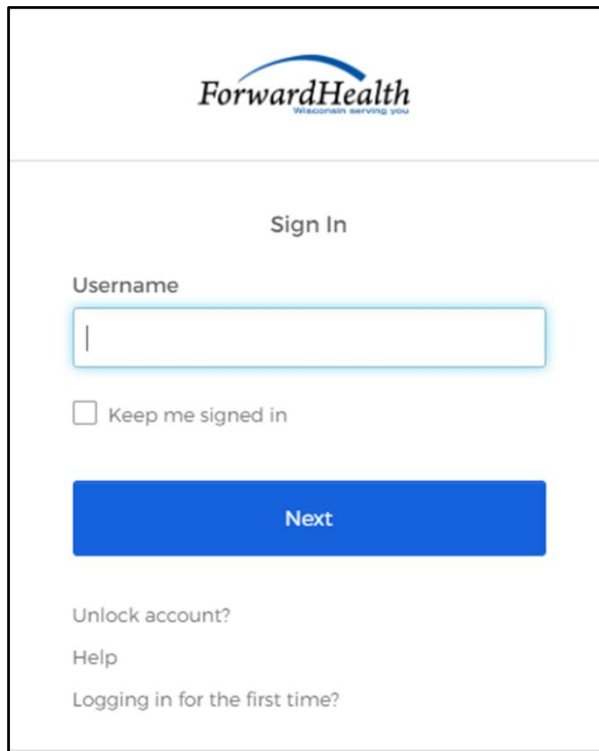


Figure 1 Children's Incident Tracking and Reporting (CITR) Login Page

2. Click **Sign in with Okta**.

A Sign In box will be displayed.



The screenshot shows a sign-in interface for ForwardHealth. At the top is the ForwardHealth logo with the tagline "Wisconsin serving you". Below the logo is a horizontal line, followed by the text "Sign In". Underneath is a "Username" label and a text input field. Below the input field is a checkbox labeled "Keep me signed in". A large blue button labeled "Next" is positioned below the checkbox. At the bottom of the form are three links: "Unlock account?", "Help", and "Logging in for the first time?".

Figure 2 Sign-In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.

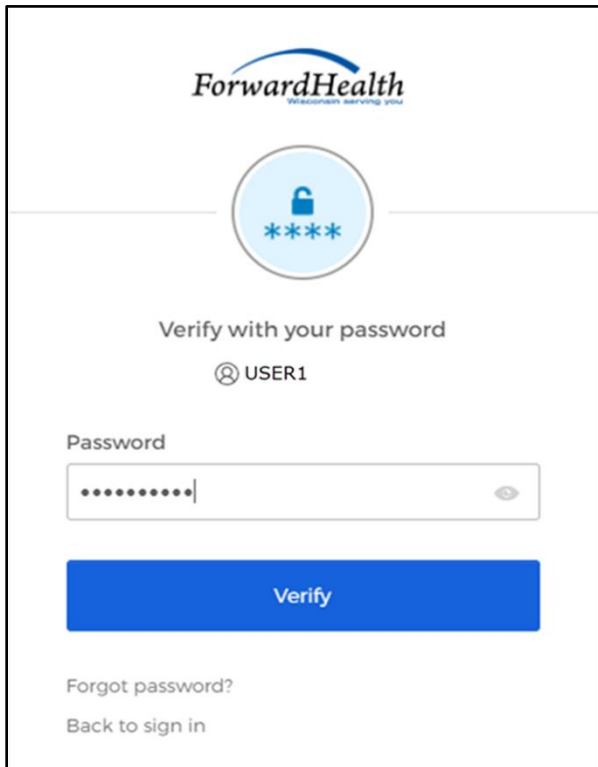


Figure 3 Verify With Your Password Box

5. Enter the user’s password. Note: If the user’s password expires when setting up MFA, a change password box will be displayed, and the user will be prompted to enter and re-enter their new password.
6. Click **Verify**.

A Get a verification email box will be displayed.

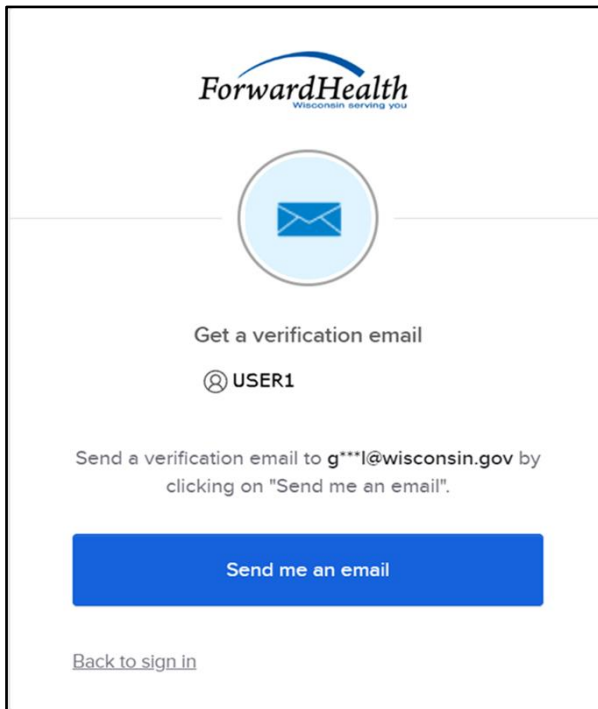


Figure 4 Get a Verification Email Box

7. Click **Send me an email**.

A box will be displayed indicating the email has been sent with a link to enter the code from the email.

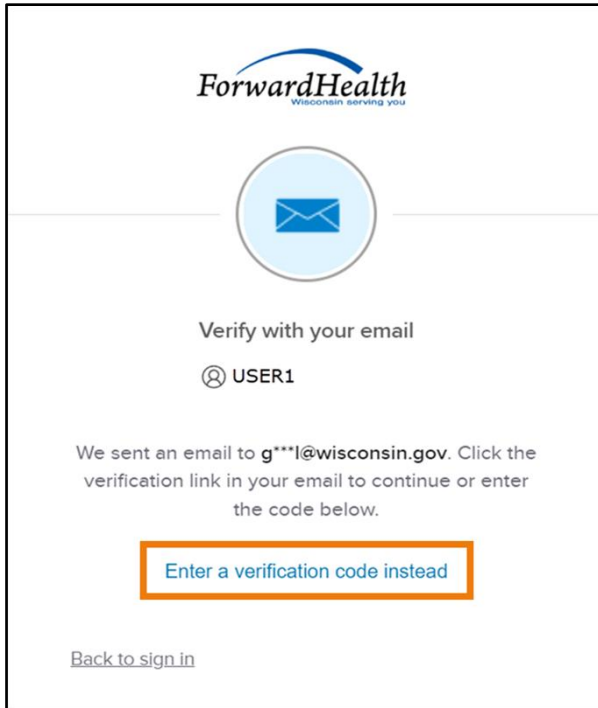


Figure 5 Verify With Your Email Box

- 8. The email with the verification code sent to the user’s email address also includes a Sign In link.

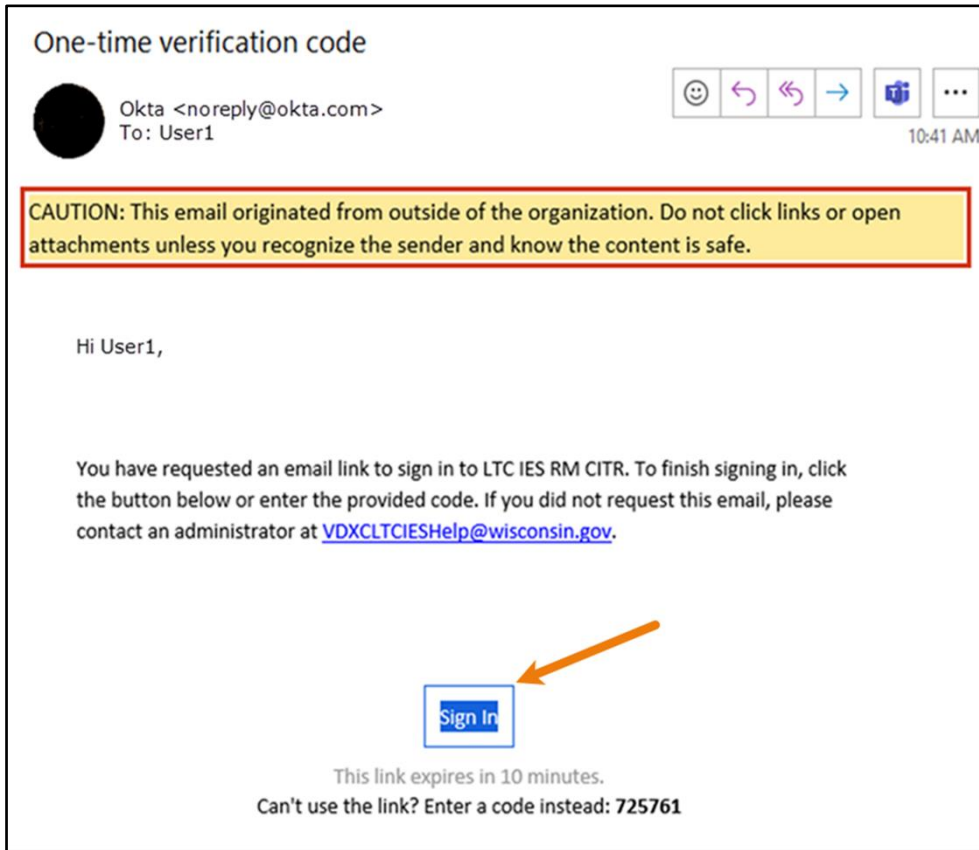


Figure 6 One-Time Verification Code Email

9. The user can choose to either:

- Click the **Sign In** link from the email.
- Capture the verification code in the email, return to the browser window, and click **Enter a verification code instead**. Enter the code from the email and click **Verify**.

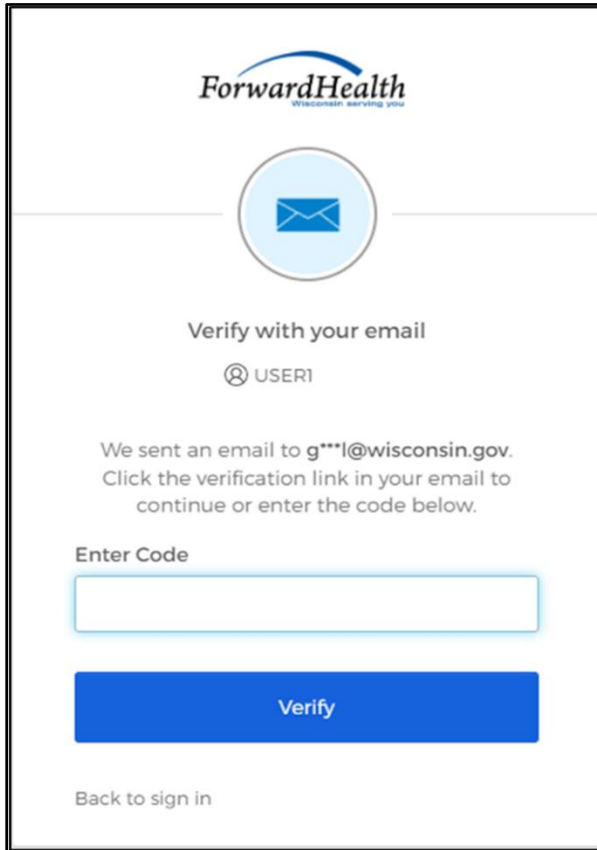


Figure 7 Verify With Your Email Box

A Set up security methods box will be displayed.

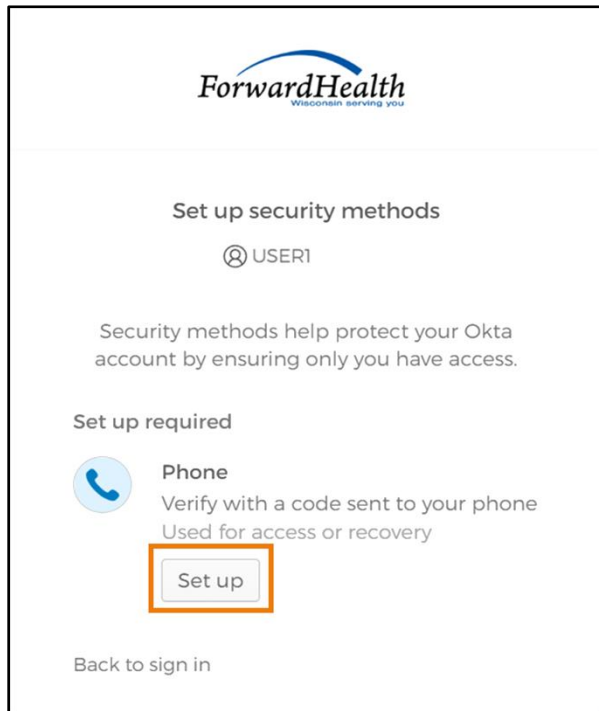


Figure 8 Set Up Security Methods Box

10. Click **Set up**.

A Set up phone authentication box will be displayed.

ForwardHealth
Wisconsin, serving you

Set up phone authentication

USER1

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

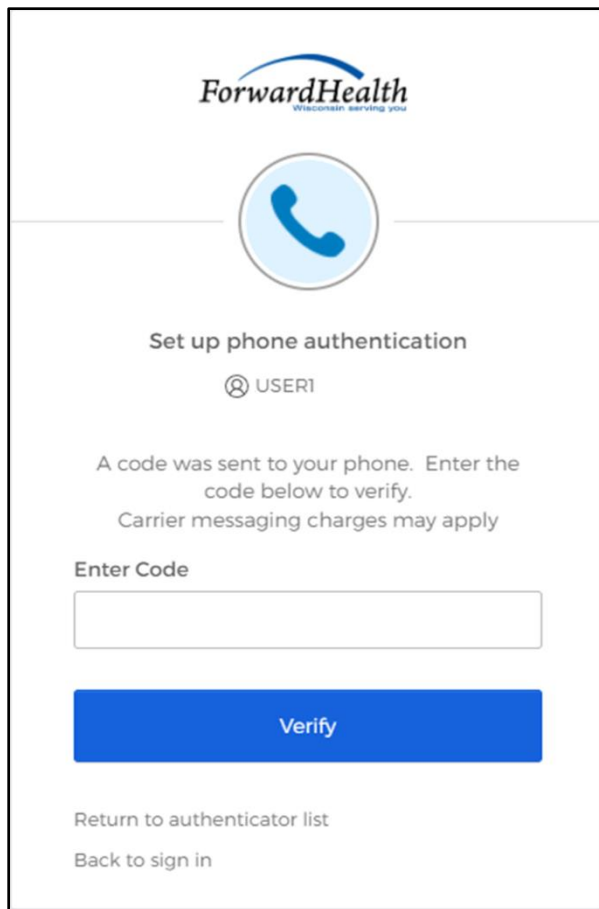
[Return to authenticator list](#)

[Back to sign in](#)

Figure 9 Set Up Phone Authentication Box

11. Select **SMS** or **Voice call** for the phone authentication method.
12. Enter the phone number.
13. Click **Receive a code via SMS** or **Receive a code via Voice call** depending on which option is selected.

A Set up phone authentication box will be displayed.



ForwardHealth
Wisconsin serving you

Set up phone authentication

USER1

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

Enter Code

Verify

[Return to authenticator list](#)

[Back to sign in](#)

Figure 10 Set Up Phone Authentication Box

14. Enter the code that was sent via text or voice call in the **Enter Code** box.
15. Click **Verify**.

A Set up security methods box will be displayed.

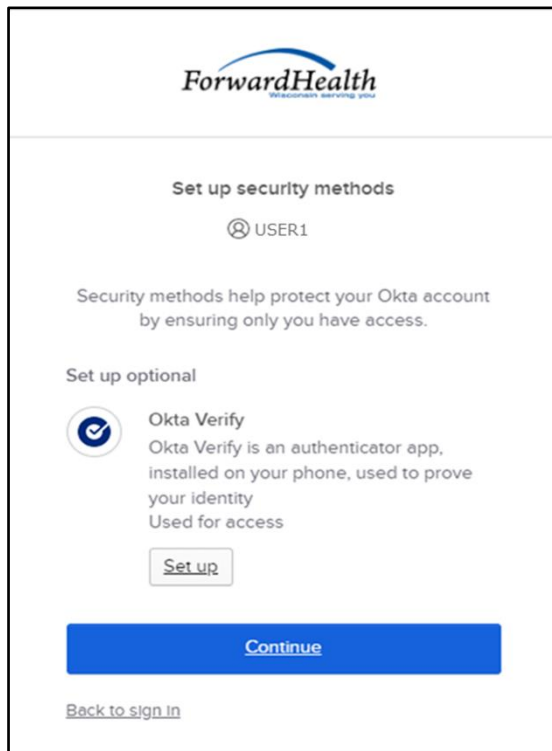


Figure 11 Set Up Security Methods Box

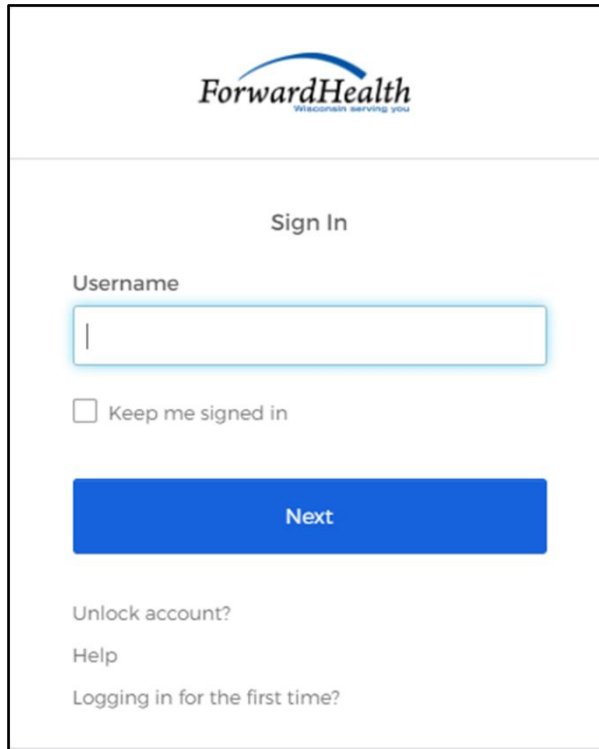
16. Click **Continue**.

17. MFA will be set up and the user will be signed in to the CITR application.

3.1 Reset Password

1. Access the CITR application.
2. Click **Sign in with Okta**.

A Sign In box will be displayed.



ForwardHealth
Wisconsin serving you

Sign In

Username

Keep me signed in

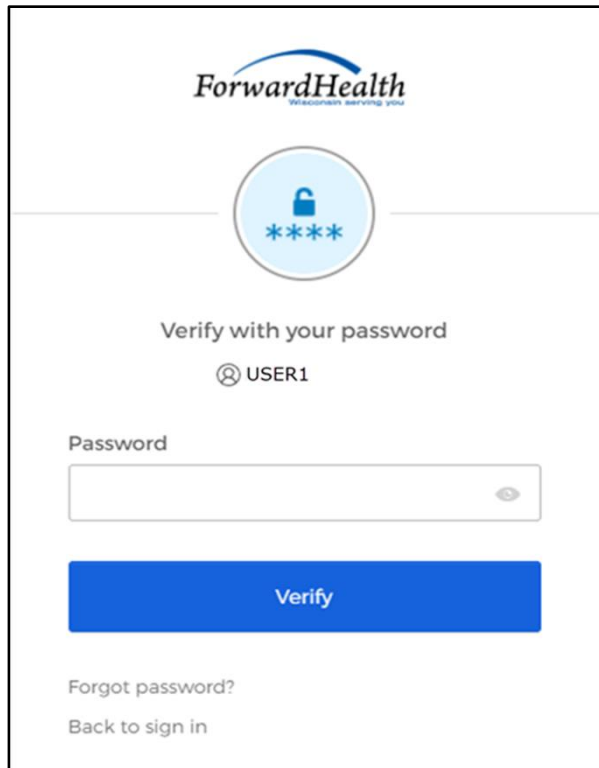
Next

Unlock account?
Help
Logging in for the first time?

Figure 12 Sign In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.



The screenshot shows the ForwardHealth login interface. At the top is the ForwardHealth logo with the tagline 'PROGRESS THROUGH CARE'. Below the logo is a circular icon containing a padlock and four asterisks. The text 'Verify with your password' is centered below the icon. Underneath, the text 'USER1' is displayed with a user icon. A 'Password' label is positioned above a text input field. To the right of the input field is an eye icon for toggling password visibility. Below the input field is a blue 'Verify' button. At the bottom left, there are two links: 'Forgot password?' and 'Back to sign in'.

Figure 13 Verify With Your Password Box

5. Click **Forgot password?** Note: Do not enter a password here.

A Reset your password box will be displayed.

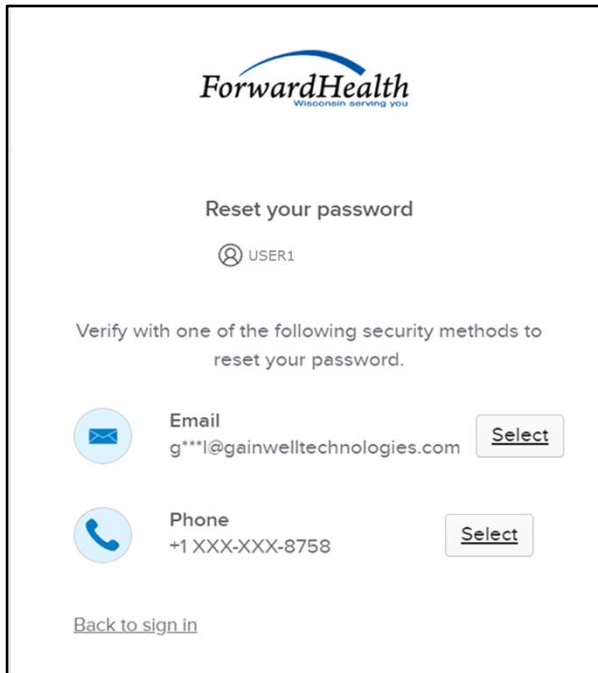


Figure 14 Reset Your Password Box

6. Click **Select** to receive a verification via email or phone.

- If the user clicks **Select** for email:
 - a. A Get a verification email box will be displayed.

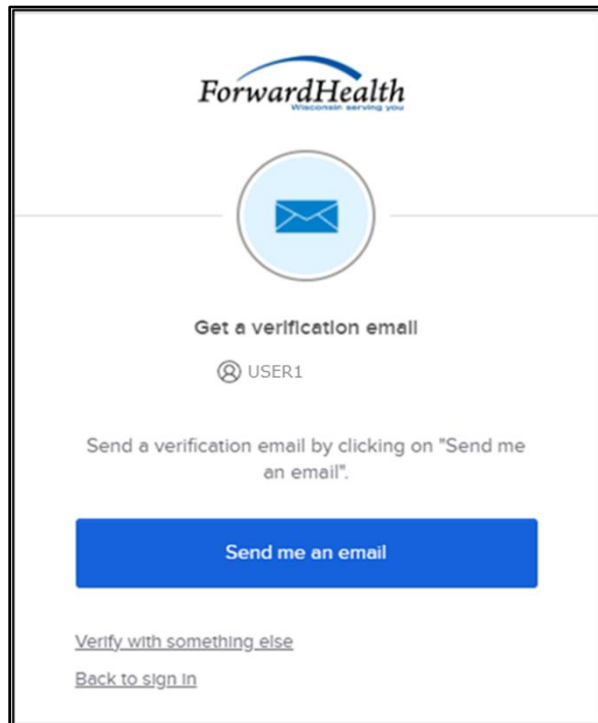


Figure 15 Get A Verification Email

- b. Click **Send me an email**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A verify with your email box will be displayed and an email will be sent.

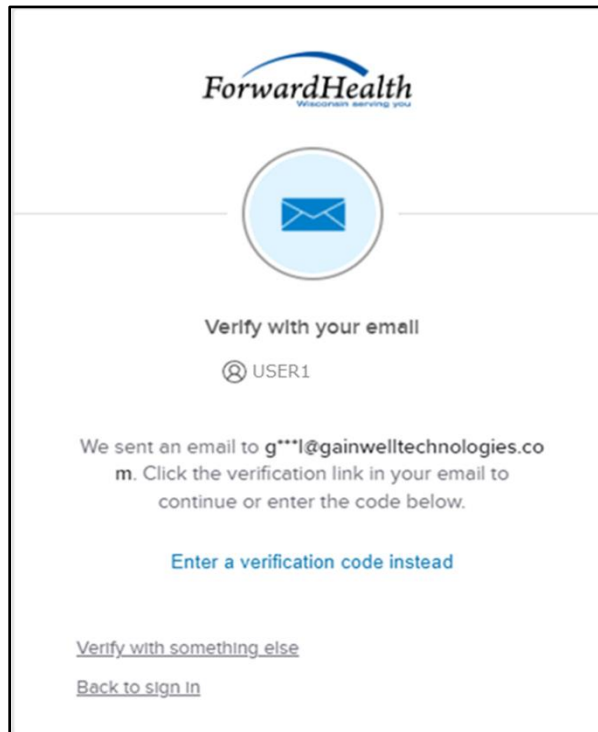


Figure 16 Verify With Your Email Box

- c. Proceed to [Step 7](#).

- If the user clicks **Select** for phone:
 - a. A verify with your phone box will be displayed.

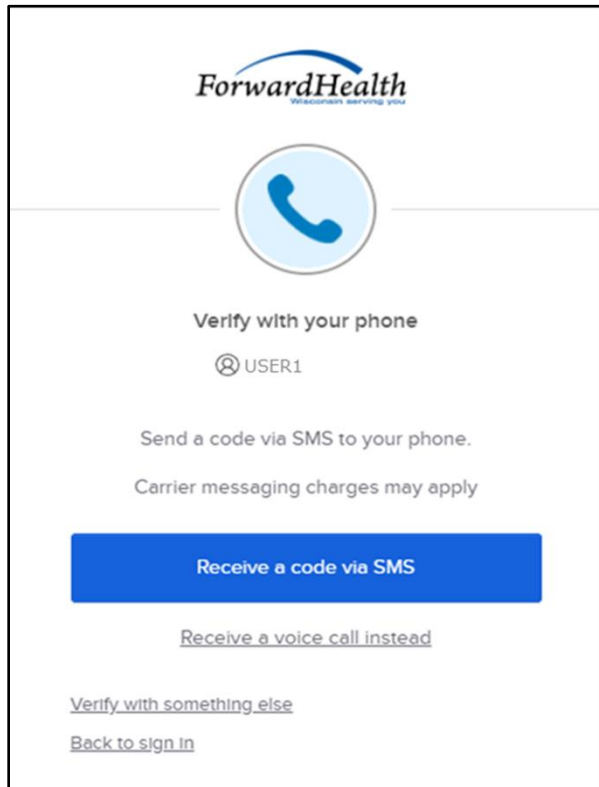
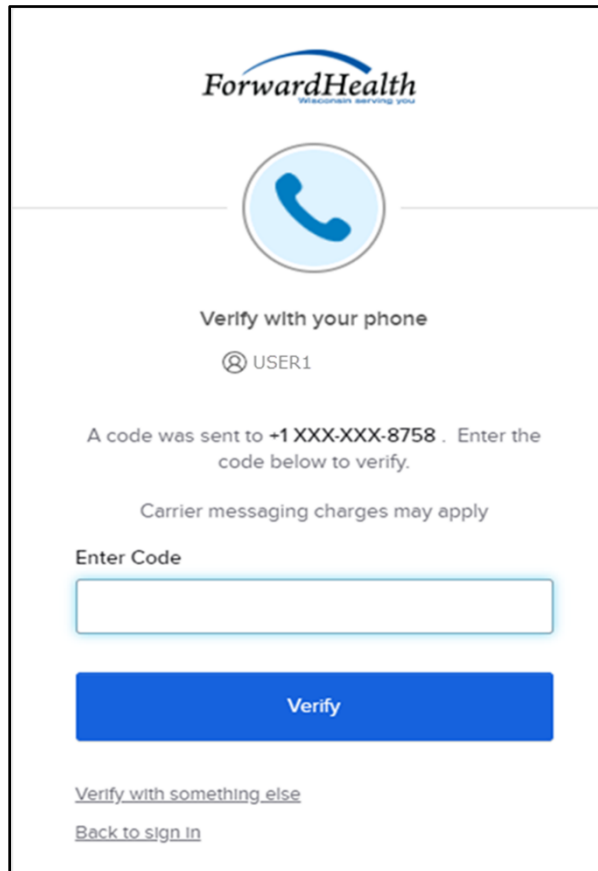



Figure 17 Verify With Your Phone Box

- b. Click **Receive a code via SMS** (text) or **Receive a voice call instead**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A Verify with your phone box will be displayed.



ForwardHealth
Wisconsin serving you



Verify with your phone

USER1

A code was sent to +1 XXX-XXX-8758 . Enter the code below to verify.

Carrier messaging charges may apply

Enter Code

Verify

[Verify with something else](#)

[Back to sign in](#)

Figure 18 Verify With Your Phone Box

- c. Enter the code that was sent.
- d. Click **Verify**.

A Get a verification email box will be displayed.

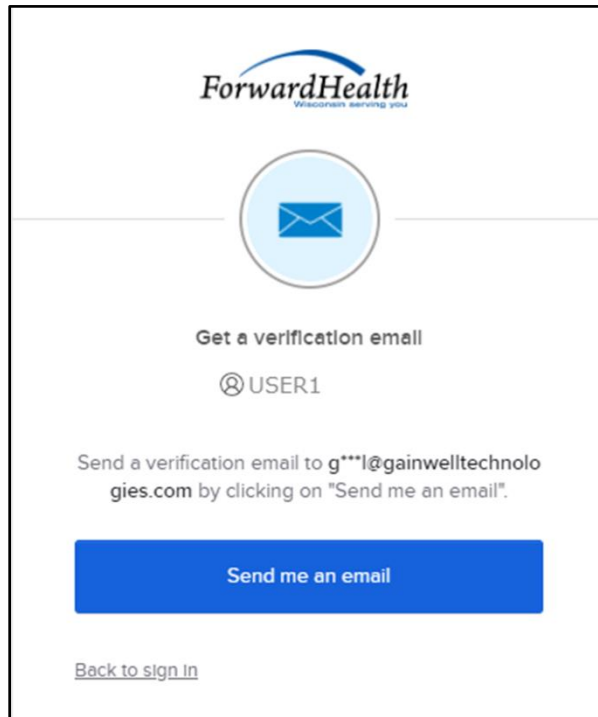


Figure 19 Get A Verification Email Box

- e. Click **Send me an email**.

A Verify with your email box will be displayed and an email will be sent.

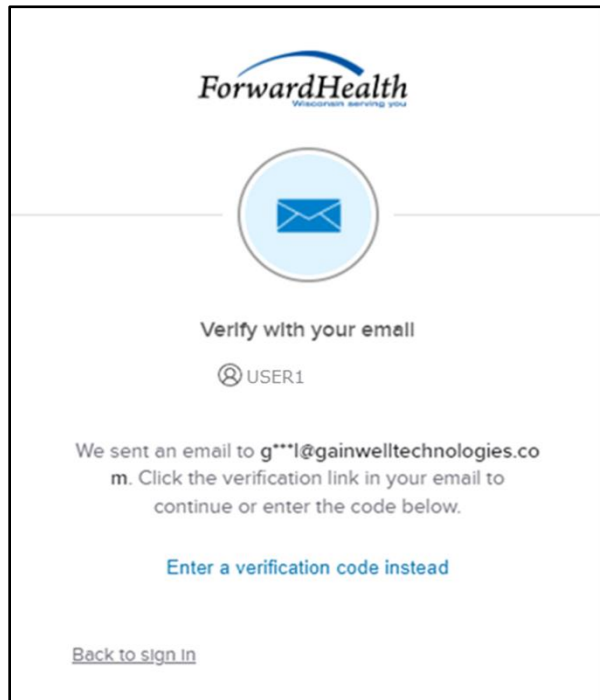


Figure 20 Verify With Your Email Box

- 7. The email sent to the user’s email address includes a **Reset Password** link (Option 1) and a verification code (Option 2).

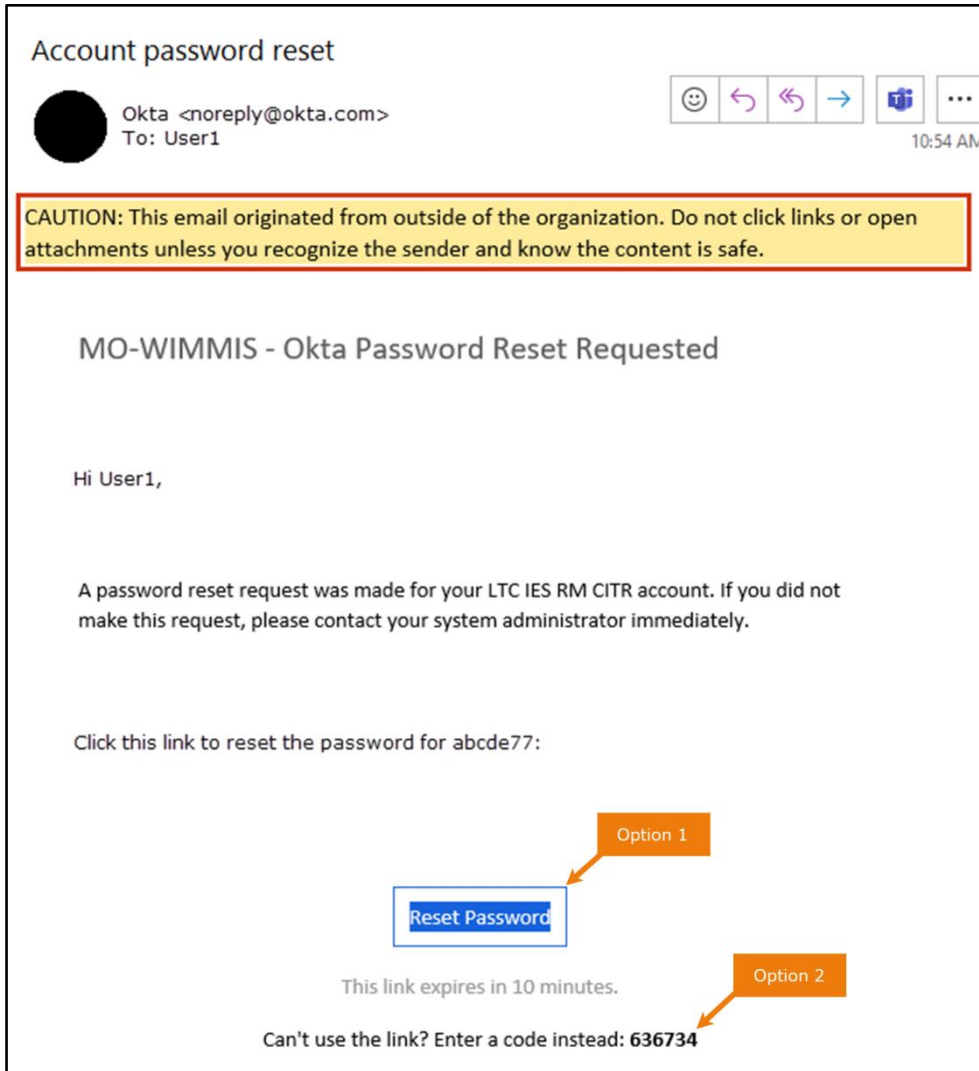


Figure 21 Account Password Reset Email

8. The user can choose to either click the **Reset Password** link (Option 1) or enter the verification code from the email (Option 2) instead.
 - Clicking the **Reset Password** link from the email will display a verification code box.

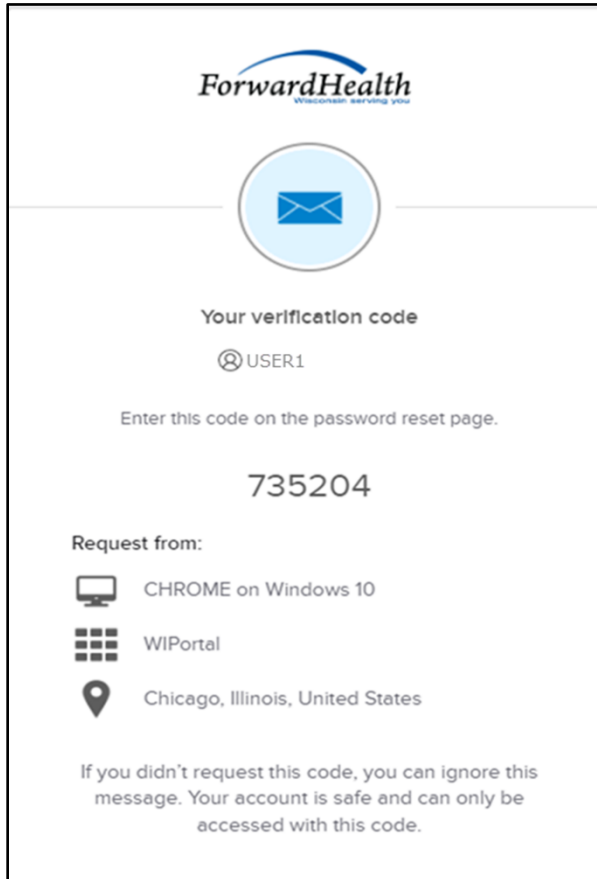


Figure 22 Verification Code Box

9. Copy the verification code from the verification code box or from the account password reset email, return to the verify with your email box, and click **Enter a verification code instead**.

- 10. Enter the code from the verification code box or the code from the account password reset email and click **Verify**.

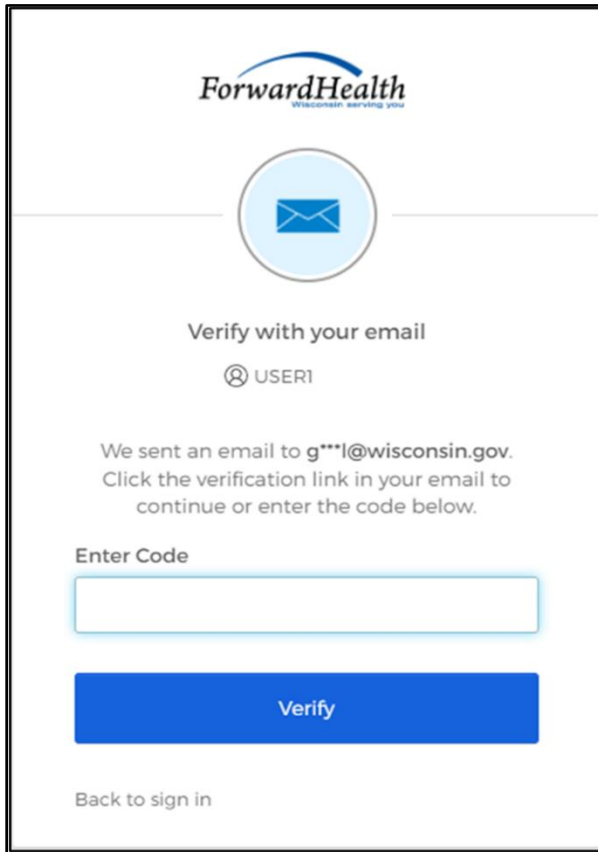
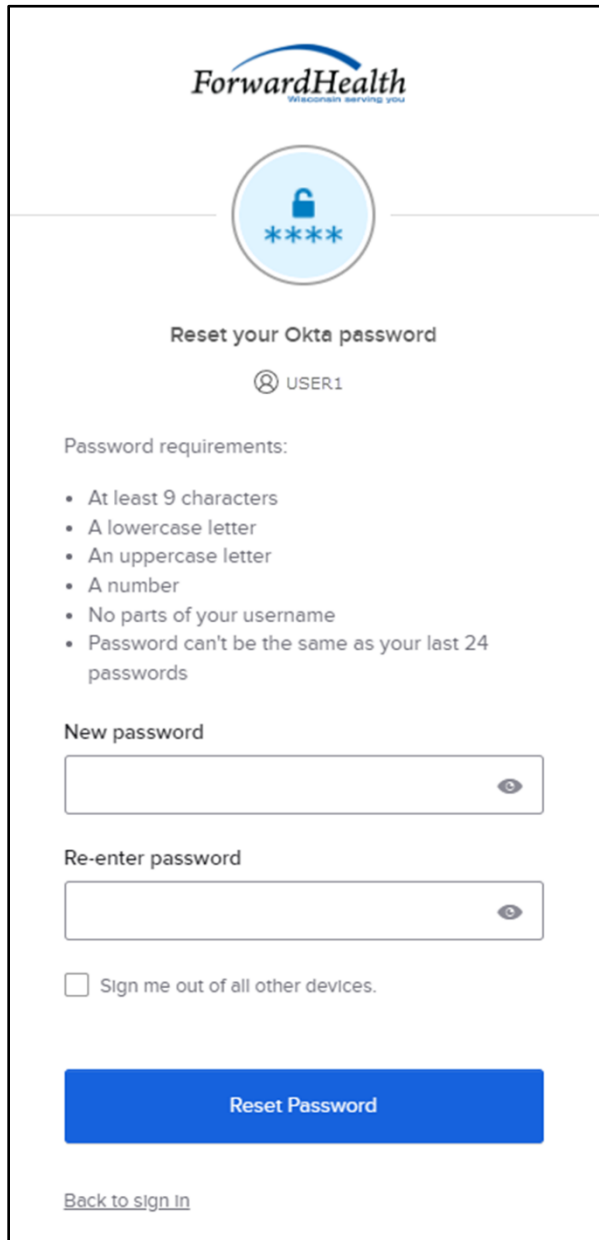


Figure 23 Verify With Your Email Box

The Reset your Okta password box will be displayed.



The screenshot shows the 'Reset your Okta password' page. At the top is the ForwardHealth logo with the tagline 'Wisconsin serving you'. Below the logo is a circular icon containing a padlock and four asterisks. The main heading is 'Reset your Okta password' followed by a user icon and the text 'USER1'. Underneath, the 'Password requirements:' section lists: At least 9 characters, A lowercase letter, An uppercase letter, A number, No parts of your username, and Password can't be the same as your last 24 passwords. There are two input fields: 'New password' and 'Re-enter password', each with a toggle icon. A checkbox labeled 'Sign me out of all other devices.' is present. A large blue 'Reset Password' button is at the bottom, with a 'Back to sign in' link below it.

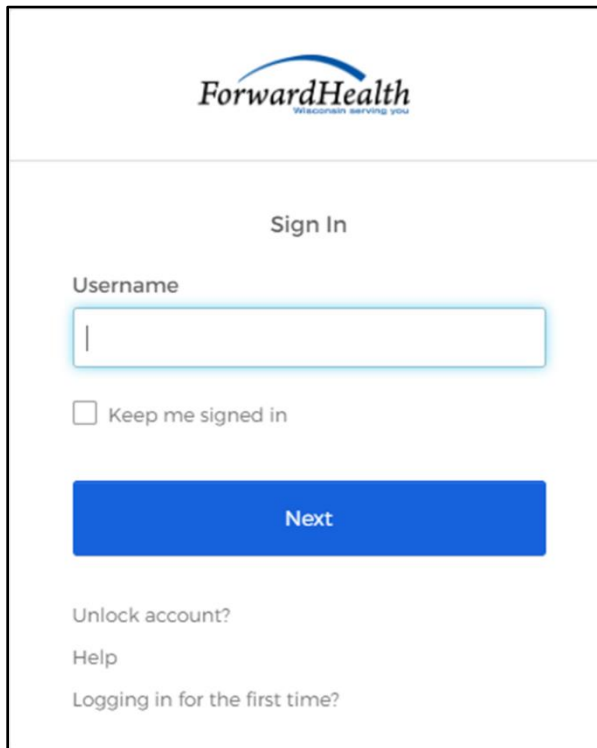
Figure 24 Reset Your Okta Password Box

11. Enter a new password (twice for confirmation).
12. Click **Reset Password**. The password will be changed and the user will be logged in to the CITR application.

3.2 Unlocking an Account

1. Access the CITR application.
2. Click **Sign in with Okta**.

A sign In box will be displayed.



ForwardHealth
Wellness working you

Sign In

Username

Keep me signed in

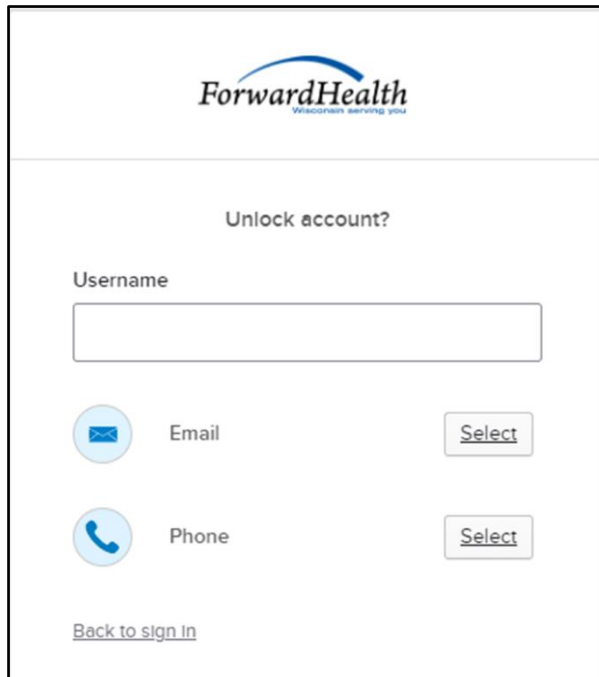
Next

Unlock account?
Help
Logging in for the first time?

Figure 25 Sign In Box

3. Click **Unlock account?**

An Unlock account box will be displayed.



The screenshot shows the ForwardHealth logo at the top, followed by the heading "Unlock account?". Below this is a "Username" label and an empty text input field. Underneath the input field are two options: "Email" with an envelope icon and a "Select" button, and "Phone" with a telephone handset icon and another "Select" button. At the bottom left of the form is a link that says "Back to sign in".

Figure 26 Unlock Account Box

4. Enter the user's username.
5. Click **Select** to receive a verification via email or phone.

- If the user clicks **Select** for email:
 - a. A Get a verification email box will be displayed.

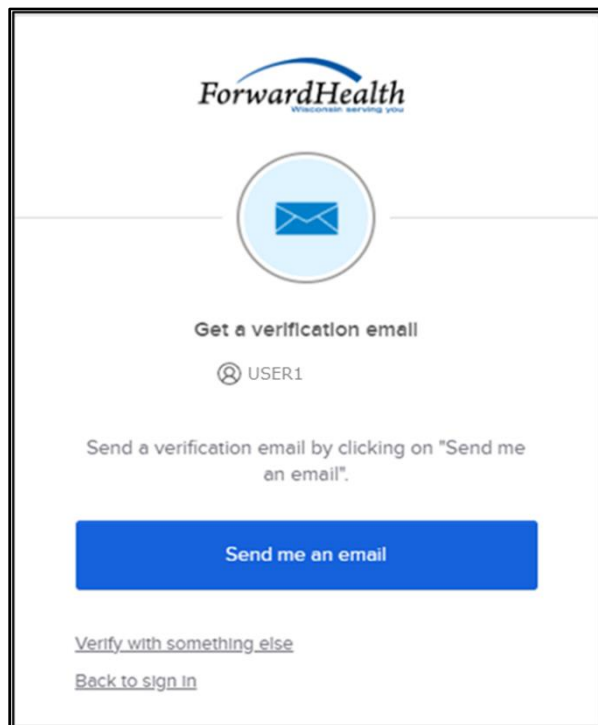


Figure 27 Get A Verification Email

- b. Click **Send me an email**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A verify with your email box will be displayed and an email will be sent.

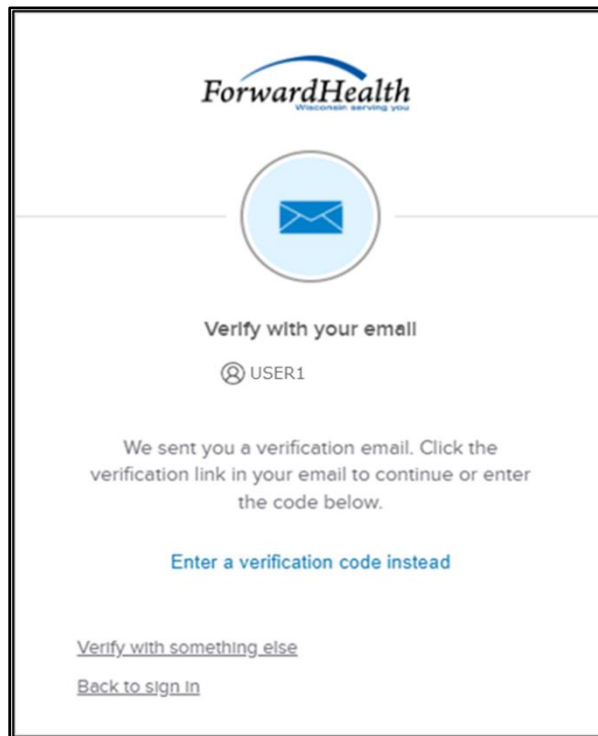


Figure 28 Verify With Your Email Box

- c. Proceed to [Step 6](#).

- If the user clicks **Select** for phone:
 - a. A verify with your phone box will be displayed.

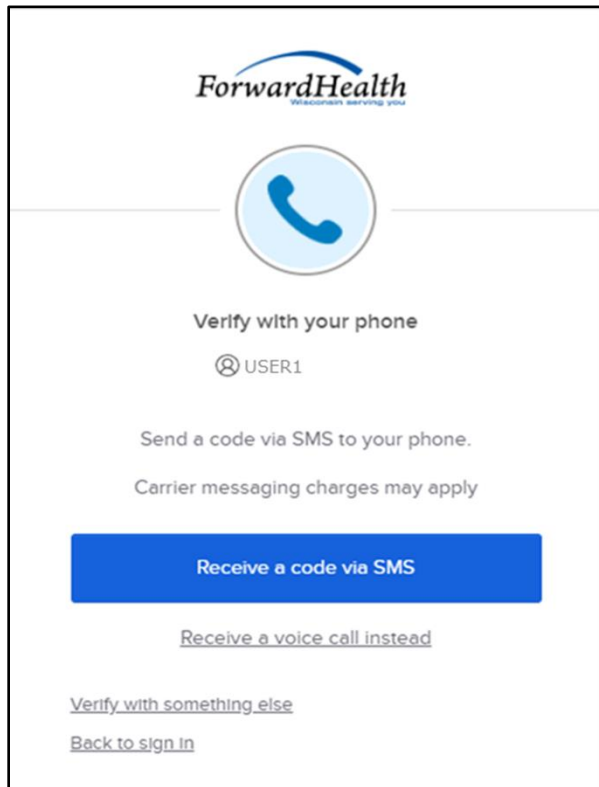
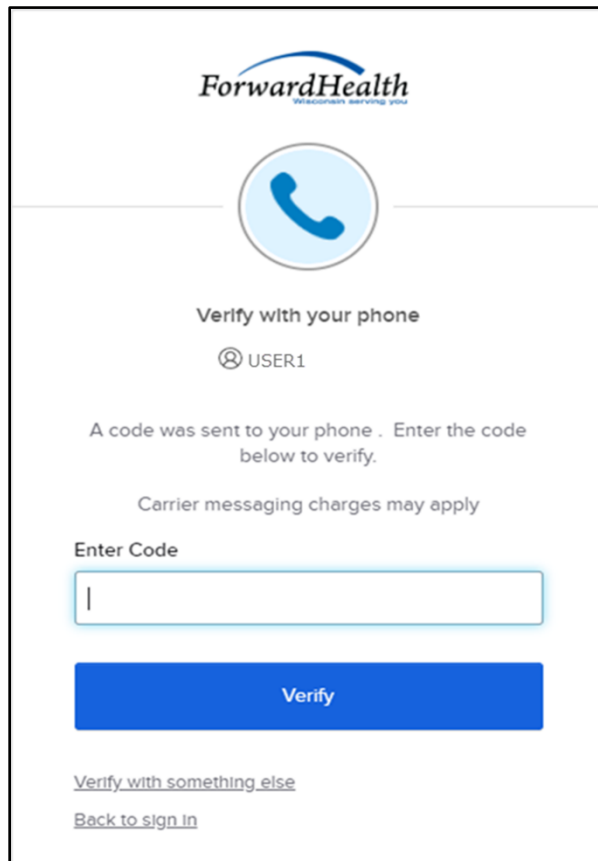


Figure 29 Verify With Your Phone Box

- b. Click **Receive a code via SMS** (text) or **Receive a voice call instead**. Note: The user also has the option to select **Verify with something else**, which will take them back to the Unlock account box, or **Back to sign in**, which will take them back to the sign in page.

A Verify with your phone box will be displayed.



ForwardHealth
REACHING SERVING YOU

Verify with your phone

USER1

A code was sent to your phone . Enter the code below to verify.

Carrier messaging charges may apply

Enter Code

Verify

[Verify with something else](#)

[Back to sign in](#)

Figure 30 Verify With Your Phone Box

- c. Enter the code that was sent.
- d. Click **Verify**.

A Get a verification email box will be displayed.

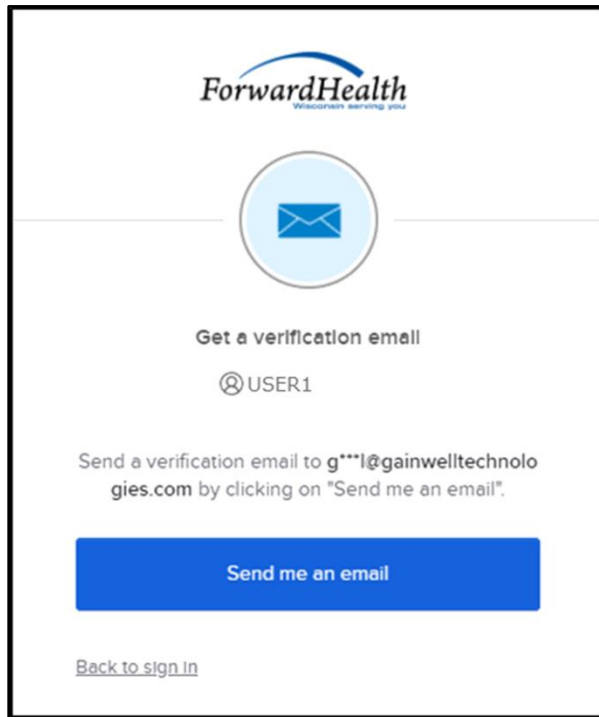


Figure 31 Get a Verification Email Box

- e. Click **Send me an email**.

A Verify with your email box will be displayed and an email will be sent.

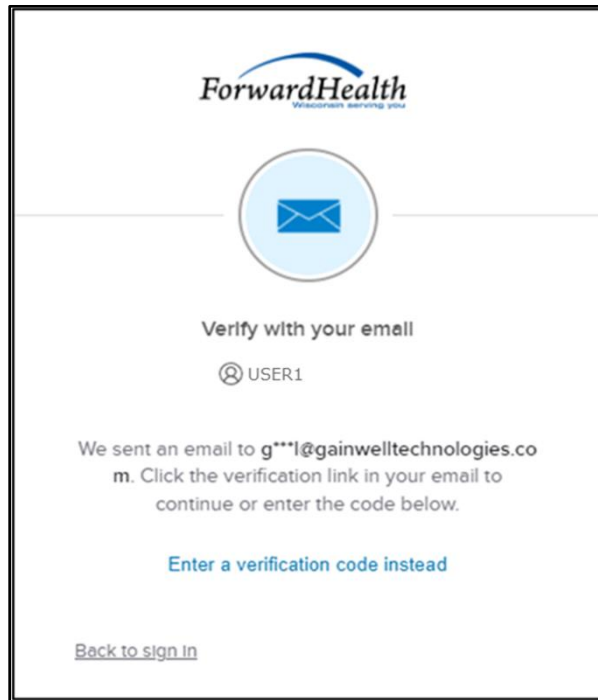


Figure 32 Verify With Your Email Box

- 6. The email sent to the user’s email address includes an **Unlock Account** link (Option 1) and a verification code (Option 2).

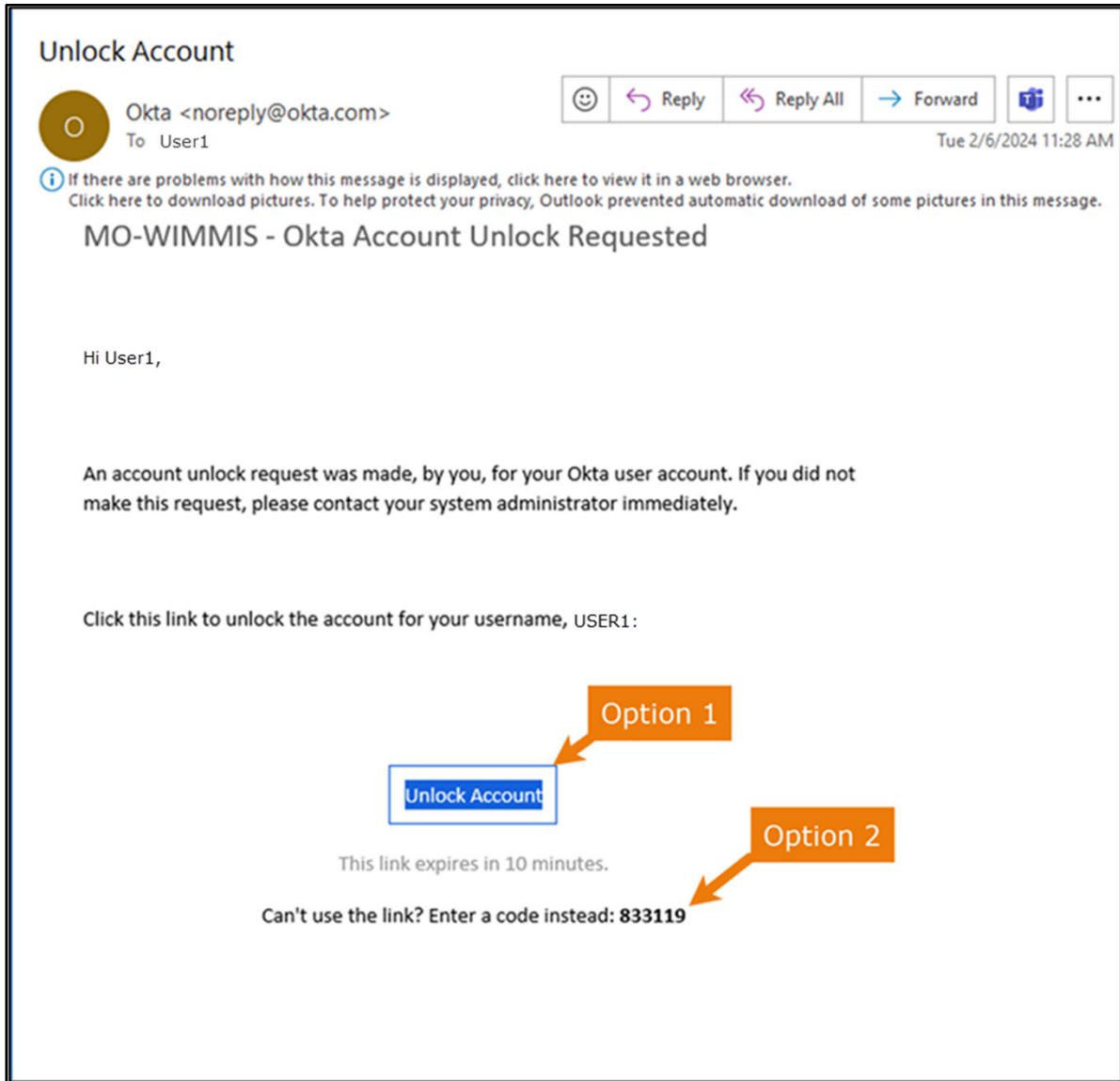


Figure 33 One-Time Verification Code Email

- 7. The user can choose to either click the **Unlock Account** link (Option 1) or enter the verification code from the email (Option 2) instead.

- Clicking the **Unlock Account** link from the email will display a verification code box.

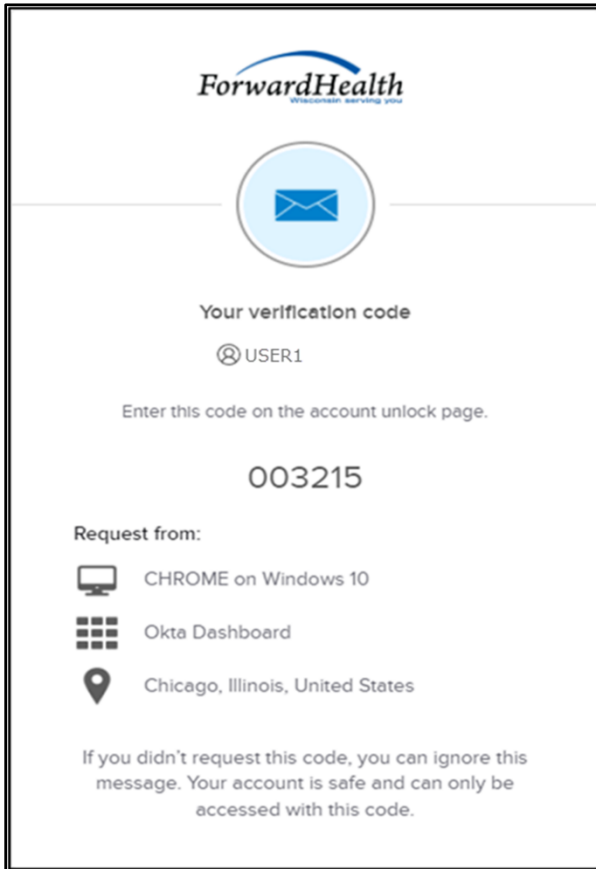


Figure 34 Verification Code Box

8. Copy the verification code from the verification code box or from the unlock account email, return to the verify with your email box, and click **Enter a verification code instead**.
9. Enter the code from the verification code box or from the unlock account email and click **Verify**.

A Verify with your password box will be displayed with a message stating the account has been successfully unlocked.

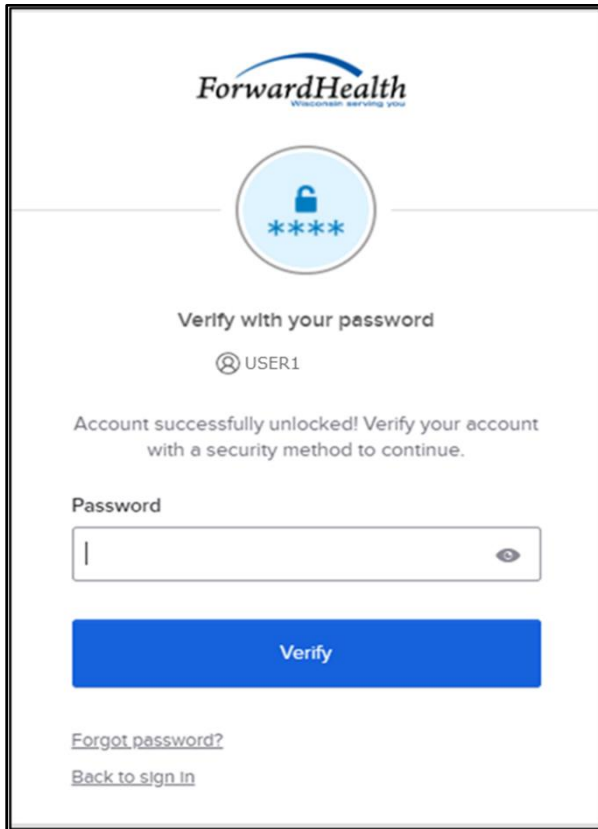


Figure 35 Verification Code Box

10. Click **Back to sign in** to log in.

4 Accessing Children's Incidents

The CITR system allows you to create an incident report that contains data concerning the incident, including attached electronic documents.

1. Access the CITR application at <https://ltcareies.forwardhealth.wi.gov/citr>.

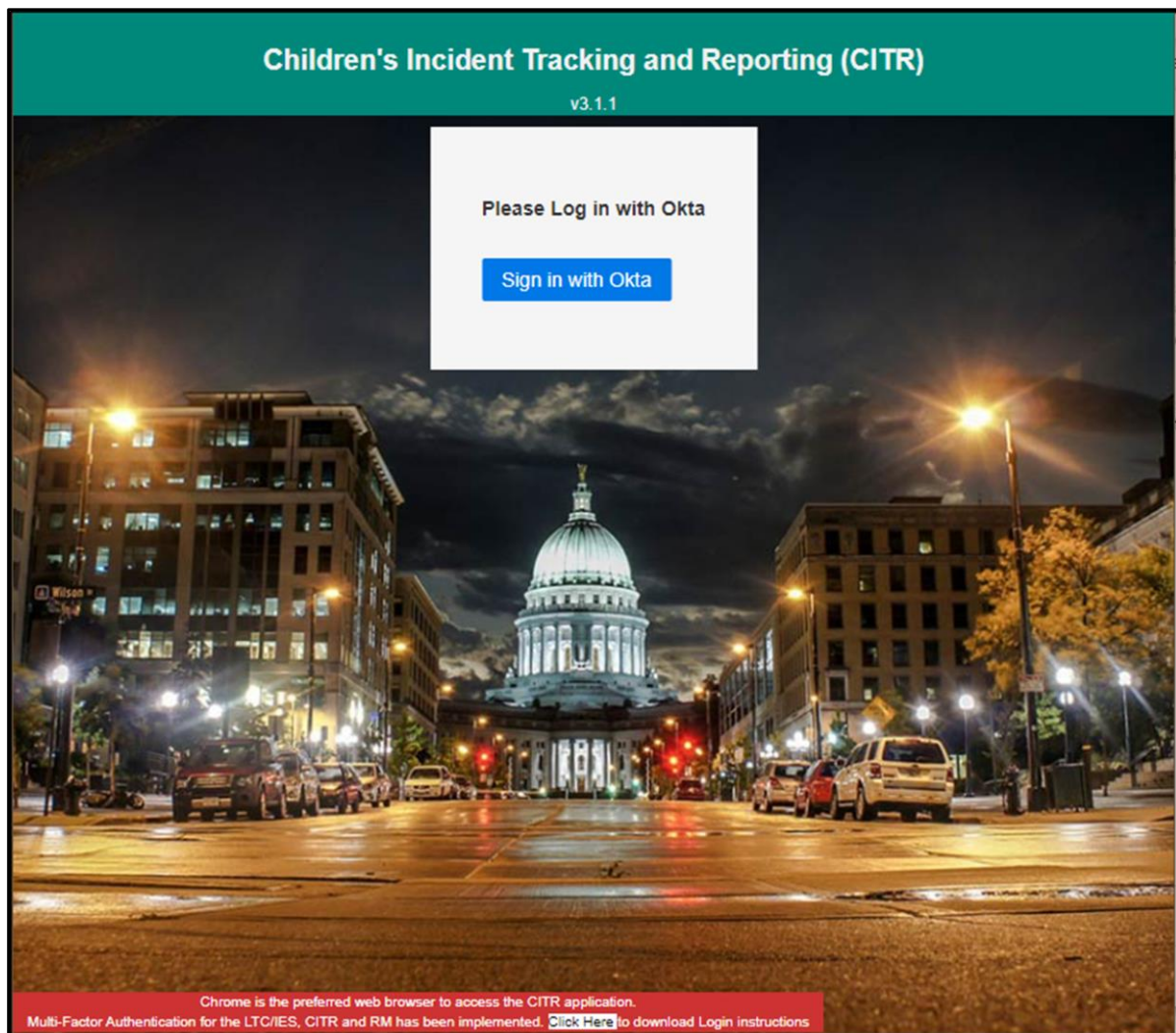
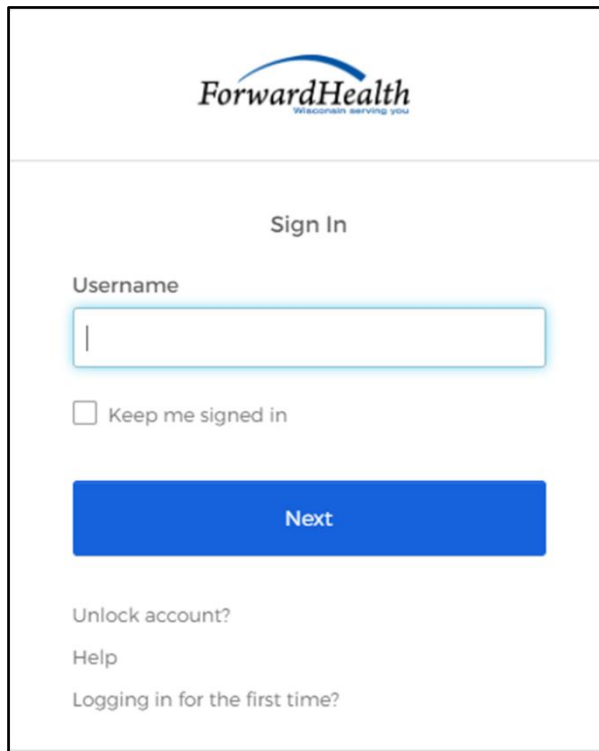


Figure 36 Children's Incident Tracking and Reporting (CITR) Sign in Page

2. Click **Sign in with Okta**.

A Sign In box will be displayed.

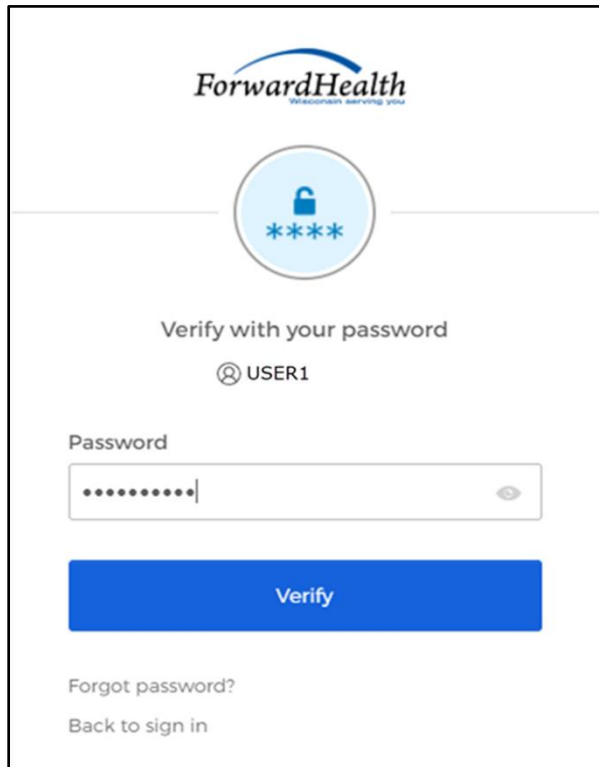


The screenshot shows a sign-in interface for ForwardHealth. At the top is the ForwardHealth logo with the tagline "Wisconsin serving you". Below the logo is a horizontal line, followed by the text "Sign In". Underneath is a "Username" label and a text input field. Below the input field is a checkbox labeled "Keep me signed in". A large blue button labeled "Next" is positioned below the checkbox. At the bottom of the form are three links: "Unlock account?", "Help", and "Logging in for the first time?".

Figure 37 Sign-In Box

3. Enter the user's username.
4. Click **Next**.

A Verify with your password box will be displayed.



ForwardHealth
Wisconsin serving you

Verify with your password

USER1

Password

Verify

Forgot password?

Back to sign in

Figure 38 Verify With Your Password Box

5. Enter the user's password. Note: If the user's password expires when setting up MFA, a change password box will be displayed, and the user will be prompted to enter and re-enter their new password.
6. Click **Verify**.

A Get a verification email box will be displayed.

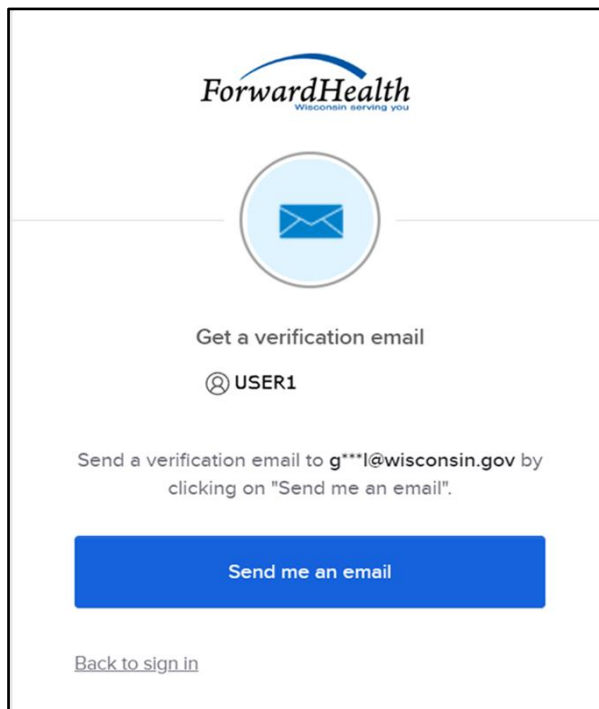


Figure 39 Get a Verification Email Box

7. Click **Send me an email**.

A box will be displayed indicating the email has been sent with a link to enter the code from the email.

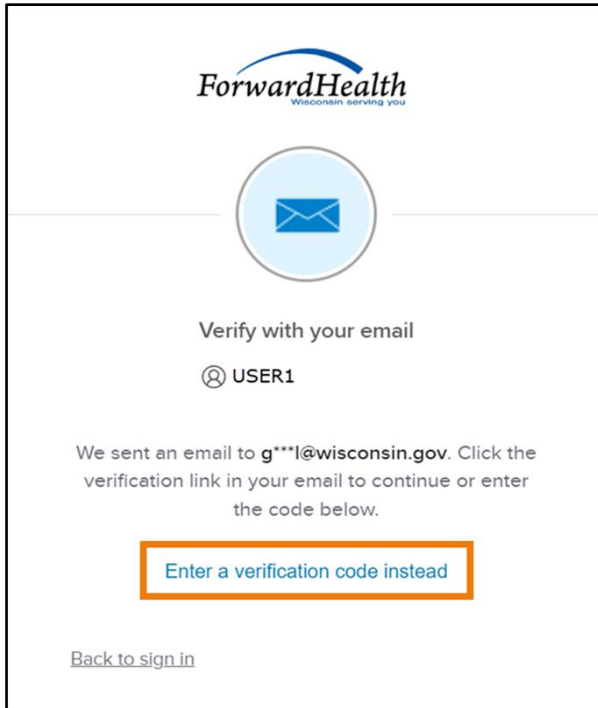


Figure 40 Verify With Your Email Box

- 8. The email with the verification code sent to the user’s email address also includes a **Sign In** link.

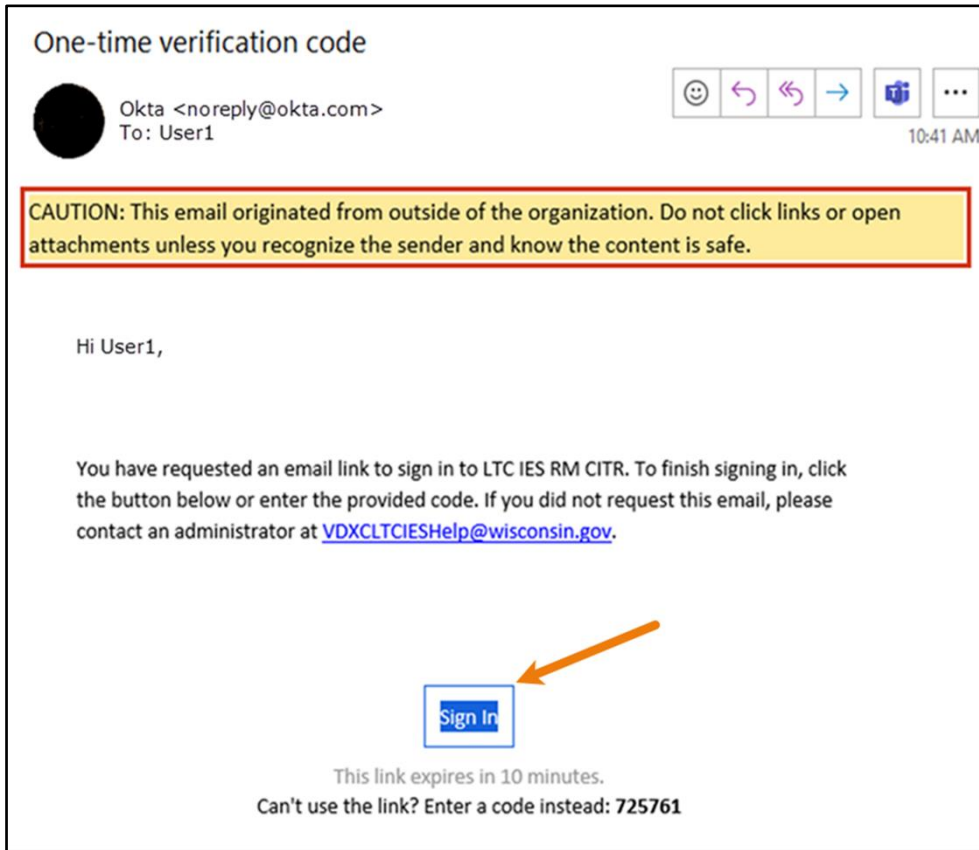


Figure 41 One-Time Verification Code Email

- 9. The user can choose to either click the **Sign In** link or enter the verification code from the email instead.

- Clicking the **Sign In** link from the email will display a verification code box.

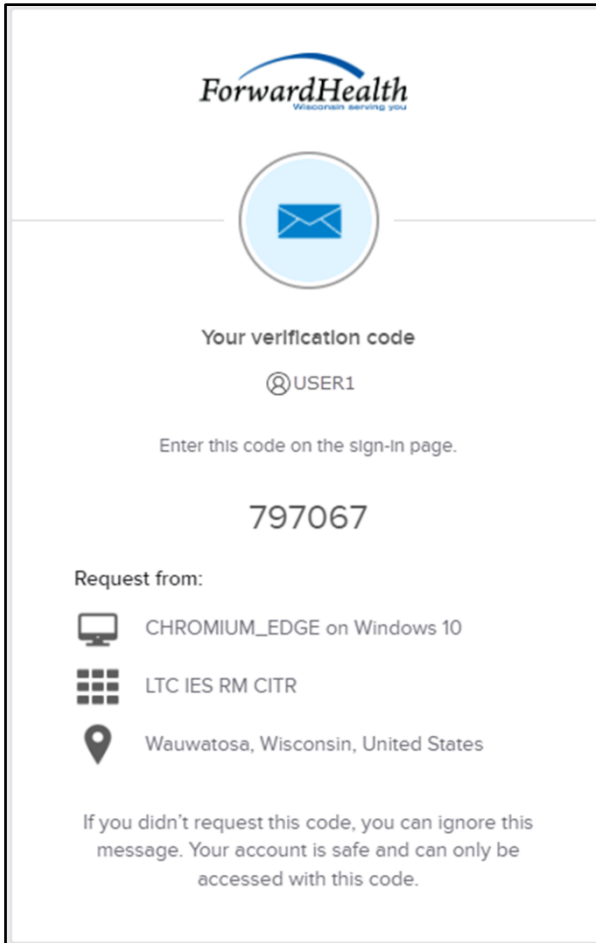


Figure 42 Verification Code Box

10. Copy the verification code from the verification code box or from the one-time verification code email, return to the verify with your email box, and click **Enter a verification code instead**.

- 11. Enter the code from the verification code box or the code from the one-time verification code email and click **Verify**.

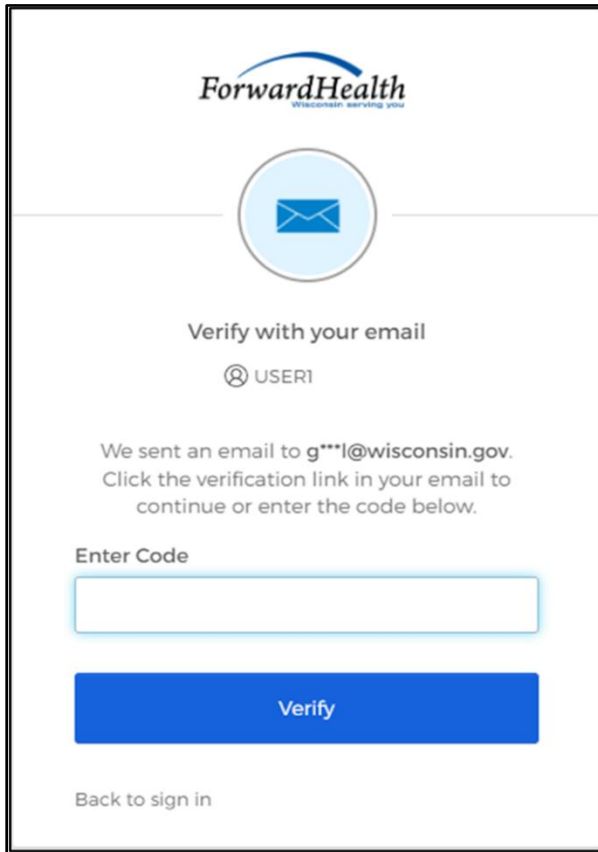


Figure 43 Verify With Your Email Box

The Incidents Dashboard will be displayed. This panel allows the user to view all the incidents that have been created for their agency. Users can search for any field displayed on this panel. By selecting the incident, the user can view and edit the data entered.

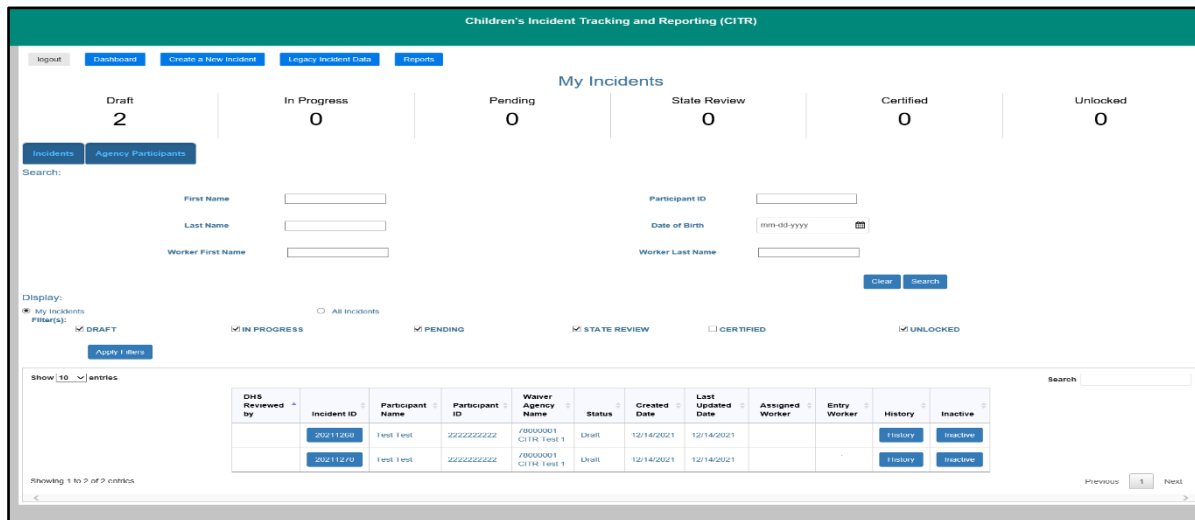


Figure 44 Incidents Dashboard

At the top of the panel are the number of incidents that are being drafted, currently in progress, pending, being reviewed by the State, certified, or unlocked.

- To view incidents, click the **My Incidents** or **All Incidents** radio button listed under the Display heading of the panel. Information about each incident created for the agency will be displayed across 12 columns at the bottom of the page. The My Incidents radio button

displays specific incidents assigned to the agency worker. The All Incidents radio button displays all the incidents for the agency.

The user can select the number of entries they want to view on each page by selecting the **Show entries** drop-down menu. The user can choose to search 10, 25, 50, or 100 entries per page.

Note: The State user has access to every incident created in the system, while the agency worker can access only reports for their agency.

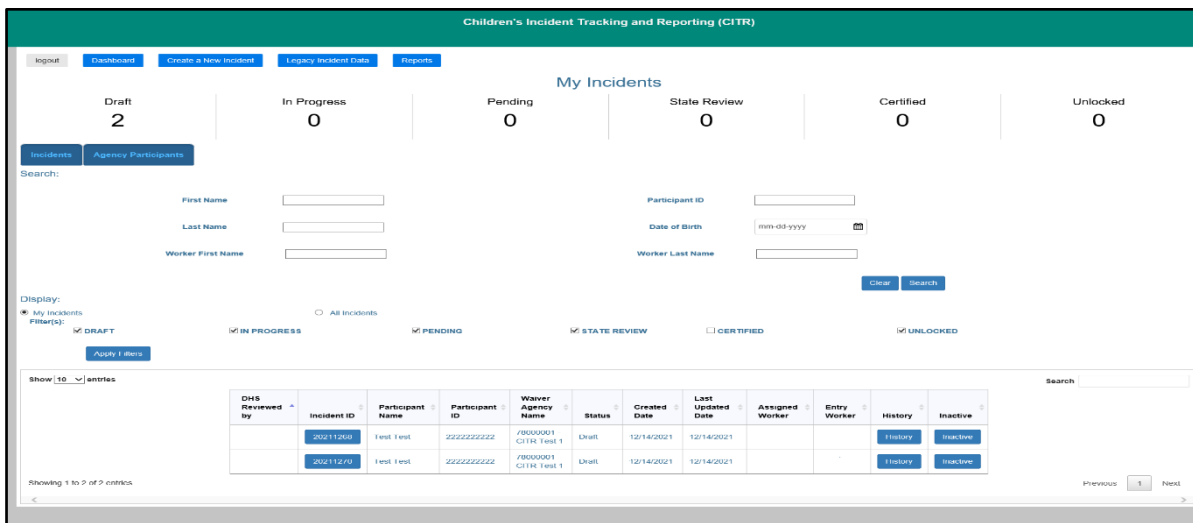


Figure 45 Incidents Dashboard

The panel will include the following information related to the incident:

- The *DHS Reviewed By* column: Used by DHS staff to indicate that an incident report has been reviewed.
- The *Incident ID* column displays the ID number of the incident. The user can click the [incident ID](#) to bring up all the information related to an incident.
- The *Participant Name* column identifies the participant.
- The *Participant ID* column displays the ID number of the participant.
- The *Waiver Agency Name* column displays the associated waiver agency.
- The *Status* column displays the status of the incident.
- The *Created Date* column displays the date the incident was created.
- The *Last Updated Date* column displays the last date the incident was updated.
- The *Assigned Worker* column displays the assigned agency worker responsible for the incident report.

- The *Entry Worker* column displays the individual who entered the information.
- The *History* column displays the participant's incident history. The user can click [History](#) to bring up the participant's incident history including all incidents and attachments.
- The *Inactive* column allows the user to inactivate the incident. The user can click the Inactive box to bring up a dialog box, which gives them the option to inactivate the incident.

Note: The user can search for any of the fields displayed on the panel by populating the **Search** box.

4.1 Search Function

The user can search for a participant incident by entering any of the following: the participant's first name, last name, ID, and/or date of birth and the agency worker's first and/or last name. The user has the option to filter incidents by choosing either the My Incidents or All Incidents radio button listed under the Display heading of the panel. Only incidents for those specific groups will be listed.

1. To search for a participant incident, enter any of the following under the "Search" section of the panel:
 - The participant's first name in the *First Name* field.
 - The participant's last name in the *Last Name* field.
 - The participant's ID in the *Participant ID* field.
 - The participant's date of birth in the *Date of Birth* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format.
 - The worker's first name in the *Worker First Name* field.
 - The worker's last name in the *Worker Last Name* field.
2. Click **Search**, and the participant's incident information will be displayed across 12 columns at the bottom of the screen.

4.2 Filter for Incidents

The user can filter for the status of incident reports by choosing from the following statuses listed at the top of the panel:

- Draft—This status indicates the incident report is still being drafted.
- In Progress—This status indicates initial notification to DHS has been made but the waiver agency has not completed the report. The status is changed from "Draft" to "In Progress" when the user selects "Save & Send to DHS" on the [Finalize Initial Save panel](#).

- Pending—If any one of the following substantiation questions from the [Final Incident Details panel](#) are answered as “Pending,” the incident status will indicate the report is pending at the final submission to DHS. When all the questions are answered with a “Yes” or “No” response, the incident will have a status of either “Certified” or “State Review” when it is submitted to DHS:
 - a. Did this incident result in a substantiated finding of abuse by a government agency?
 - b. Did this incident result in a substantiated finding of neglect by a government agency?
 - c. Did this incident result in a substantiated finding of exploitation by a government agency?

Note: When an incident has been in the status of pending for 60 days, an email will be sent warning that the user is approaching the 90-day limit and reminding them to update the incident report. Another email will be sent when an incident has been in a status of pending for 90 days and they will be reminded to update the incident report.

- State Review—This status indicates the incident report has been completed by the waiver agency and DHS is reviewing.
 - Certified—This status indicates that DHS has completed review and the incident report is complete.
 - Unlocked—This status indicates the State administrator has unlocked the incident report to allow the user to edit the incident after it has been sent to DHS. This is usually done when DHS requires additional information.
1. To filter for the status of an incident, check the box for the appropriate filter(s).
 2. Filters will be applied when selected or when the user clicks **Apply Filters**. All incidents with the status indicated will be displayed.

4.3 Participant Incident History

This panel allows a user to view the participant's incident history. The incident history can also be accessed via the [Agency Participants dashboard](#).

1. On the Incidents dashboard, click **History** in the History column for an agency participant. The Participant Incident History panel will be displayed.

Participant INCIDENT HISTORY

Participant ID: 1212121212 First Name: Middle Initial Name: Last Name: Suffix: DATE OF BIRTH:

INCIDENTS & ASSOCIATED ATTACHMENTS

Legacy History Show 10 entries Search:

	Incident ID	Incident Type	Agency	Incident Status	Date Occurred
Attachments (3)	2019204	Behavioral		Draft Application	11-SEP-2019

Showing 1 to 1 of 1 entries Previous 1 Next

Figure 46 Participant Incident History Panel

The panel may include the following information related to the participant:

- The *Participant ID* field displays the participant's ID number.
- The *First Name* field displays the participant's first name.
- The *Middle Initial Name* field displays the participant's middle initial.
- The *Last Name* field displays the participant's last name.
- The *Suffix* field displays the participant's suffix, if applicable
- The *Date of Birth* field displays the participant's date of birth.

The "Incidents & Associated Attachments" section may include the following information:

- The *Incident ID* column displays the ID number of the incident.
- The *Incident Type* column displays the type of incident.
- The *Agency* column identifies the responsible agency.
- The *Incident Status* column displays the status of the incident.
- The *Date Occurred* column displays the date the incident occurred.

Note: Users can click **Attachments** in the first column under the "Incidents & Associated Attachments" section to view a list of associated attachments related to the incident. Information may include the attachment name, URL, type, and uploaded date.

Note: Users can search for a participant's incident history by entering an incident ID in the **Search** box.

4.4 Inactivating an Incident

This panel allows a user to inactivate an incident. Only incidents that are in a status of "Draft" or "In Progress" can be inactivated.

1. On the Incidents dashboard, click **Inactive** in the Inactive column for an agency participant. A dialog box will appear to confirm that the user wants to inactivate the incident.

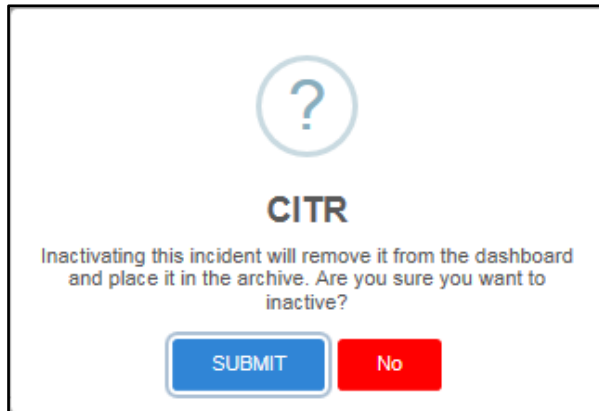


Figure 47 Dialog Box

2. Click **SUBMIT**. A dialog box will appear to indicate the incident has been set inactive.

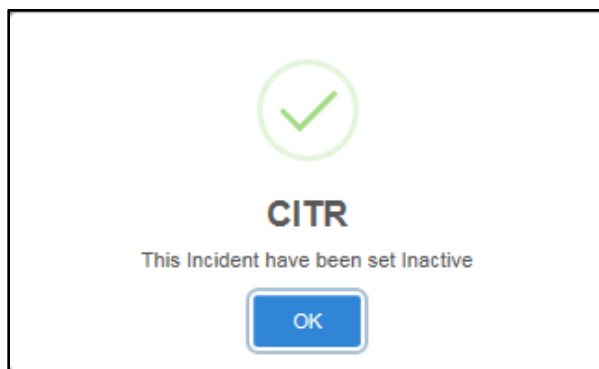


Figure 48 Dialog Box

3. Click **OK**. The Incidents dashboard will be displayed.

4.5 Agency Participants Dashboard

This panel allows the user to view all agency participants and search/filter through the data. The user can create a new incident for one of the participants. When the user clicks the Create Incident button associated with the participant, the participant data is prefilled on the first form.

1. On the Incidents dashboard, click **Agency Participants**. The Agency Participants dashboard will be displayed.

The screenshot shows the 'Agency Participants' dashboard within the CITR system. At the top, there is a navigation bar with 'logout', 'Dashboard', 'Create a New Incident', 'Legacy Incident Data', and 'Reports'. Below this, the dashboard title 'Agency Participants' is centered. A summary row displays incident counts: Draft (10), In Progress (0), Pending (0), State Review (1), Certified (0), and Unlocked (0). Below the summary, there are two tabs: 'Incidents' and 'Agency Participants'. A search section follows, with a 'Search:' label and four input fields: 'First Name', 'Last Name', 'Participant ID', and 'Date of Birth' (with a calendar icon). A 'Search' button is located at the bottom right of the search section.

Figure 49 Agency Participants Dashboard

At the top of the panel are the number of incidents that are being drafted, currently in progress, pending, being reviewed by the State, certified, or unlocked.

4.5.1 Search Function

A user can search for a participant by entering any of the following: the participant's first name, last name, ID, and/or date of birth.

1. To search for a participant, enter any of the following under the "Search" section of the panel:
 - The participant's first name in the *First Name* field.
 - The participant's last name in the *Last Name* field.
 - The participant's ID in the *Participant ID* field.
 - The participant's date of birth in the *Date of Birth* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format.
2. Click **Search**. Information about each participant will be displayed across eight columns at the bottom of the screen.

Children's Incident Tracking and Reporting (CITR)

logout | Dashboard | Create a New Incident | Legacy Incident Data | Reports

Agency Participants

Draft	In Progress	Pending	State Review	Certified	Unlocked
16	0	0	1	0	0

Incidents | Agency Participants

Search:

First Name: Participant ID:

Last Name: Date of Birth:

[Search](#)

Show 10 entries Search:

Participant ID	Participant Name	Date of Birth	Create Incident	View History	Last Incident Date	Enrollment Period	Status
111111111	Tester M Tested	01/25/2004	Create Incident	View	02/01/2020	03/06/2018-Current	Current
111111115	Testmaxwell Testcassy	01/28/2004	Create Incident	View	02/01/2020	10/01/2017-Current	Current

Showing 1 to 2 of 2 entries Previous | 1 | Next

Figure 50 Agency Participant Search

The panel may include the following information related to the participant:

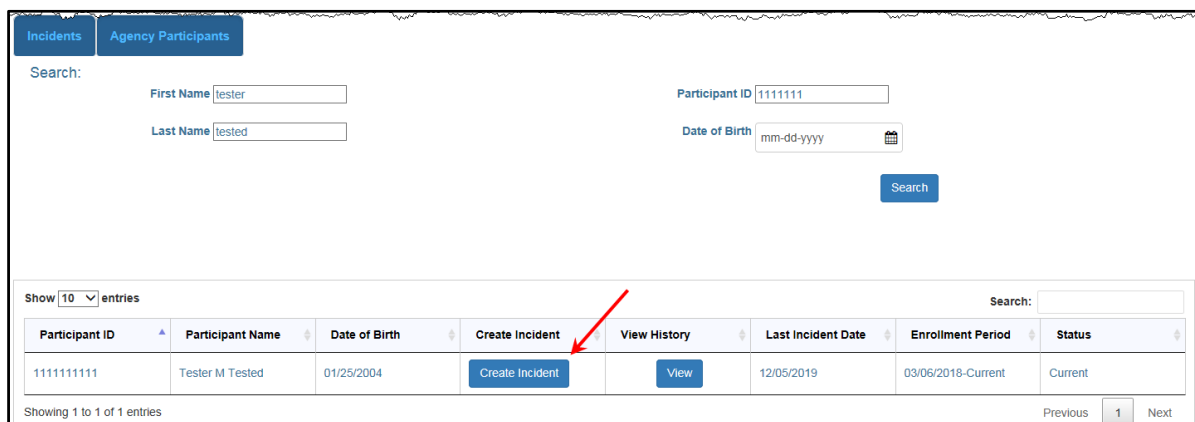
- The *Participant ID* column displays the identification number of the participant.
- The *Participant Name* column identifies the participant.
- The *Date of Birth* column displays the participant’s date of birth.
- The *Create Incident* column allows the user to create an incident by clicking the [Create Incident](#) box.
- The *View History* column allows the user to view the prior history of the participant by clicking [View](#).
- The *Last Incident Date* column displays the last reported incident.
- The *Enrollment Period* column displays the dates the participant is enrolled.
- The *Status* column displays the status of the participant.

Note: The user can search for any of the fields displayed on the panel by populating the **Search** box.

5 Creating an Incident for a Participant Enrolled in CLTS

This function allows the user to create an incident for a participant that is currently enrolled in CLTS.

1. On the Agency Participants dashboard, search for an agency participant using the [search function](#). Input any of the following: the participant's first name, last name, ID, and/or date of birth using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format.
2. Click **Search**. Information about the participant will be displayed across eight columns at the bottom of the screen.
3. Click **Create Incident** in the Create Incident column for the agency participant.



The screenshot shows the 'Agency Participants' dashboard. At the top, there are tabs for 'Incidents' and 'Agency Participants'. Below the tabs is a search form with fields for 'First Name' (containing 'tester'), 'Last Name' (containing 'tested'), 'Participant ID' (containing '11111111'), and 'Date of Birth' (containing 'mm-dd-yyyy' and a calendar icon). A 'Search' button is located to the right of the search fields. Below the search form is a table with the following columns: 'Participant ID', 'Participant Name', 'Date of Birth', 'Create Incident', 'View History', 'Last Incident Date', 'Enrollment Period', and 'Status'. The table contains one entry for 'Tester M Tested' with ID '1111111111' and date of birth '01/25/2004'. The 'Create Incident' column for this entry has a blue button labeled 'Create Incident', which is highlighted with a red arrow. The 'View History' column has a blue button labeled 'View'. The table also includes pagination controls at the bottom: 'Showing 1 to 1 of 1 entries', 'Previous', '1', and 'Next'.

Figure 51 Figure 1 Create Incident

4. A dialog box will appear to confirm the user's selection.

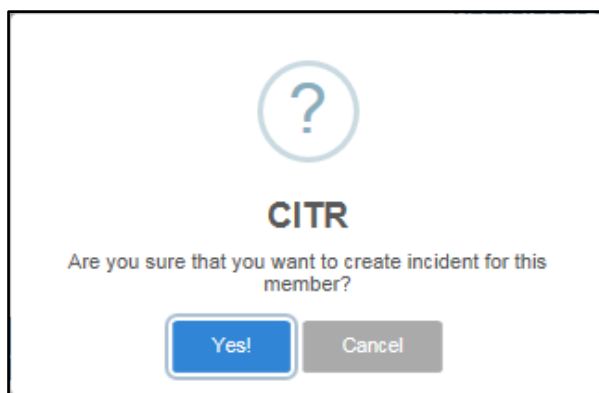


Figure 52 Dialog Box

- Click **Yes!** The Participant Information and Incident Notification panel will be displayed under the Notification stage.

The screenshot displays the CITR web application interface. At the top, there is a navigation bar with 'logout', 'Dashboard', 'Create a New Incident', 'Legacy Incident Data', and 'Reports'. Below this is a header for 'Children's Incident Tracking and Reporting (CITR)'. A progress bar shows four stages: NOTIFICATION (active), AGENCY, STATE REVIEW, and CERTIFIED. The main content area is divided into two sections: 'PARTICIPANT INFORMATION' and 'INCIDENT NOTIFICATION'. The 'PARTICIPANT INFORMATION' section includes fields for Participant ID (with a search button), First Name, Middle Initial/Name, Last Name, Suffix, Gender (Male/Female), Date of Birth, Previous First Name, Middle Initial/Name, Last Name, Target Group (IDD, SED, PD), and Program (CLTS, CCOP). The 'INCIDENT NOTIFICATION' section includes fields for Date Incident Occurred, What agency is responsible for this Participant?, Date the waiver agency was notified of Incident, In what county did the incident occur?, and Who reported the incident to the waiver agency?. A 'Download Incident' button is located at the bottom left, and a 'Save & Continue' button is at the bottom right.

Figure 53 Participant Information/Incident Notification Panel

Note: A progress header is displayed at the top of the panel. The paper icon represents the point at which initial notification to DHS has been made. The lock icon represents the point at which the final report has been submitted and can no longer be updated.

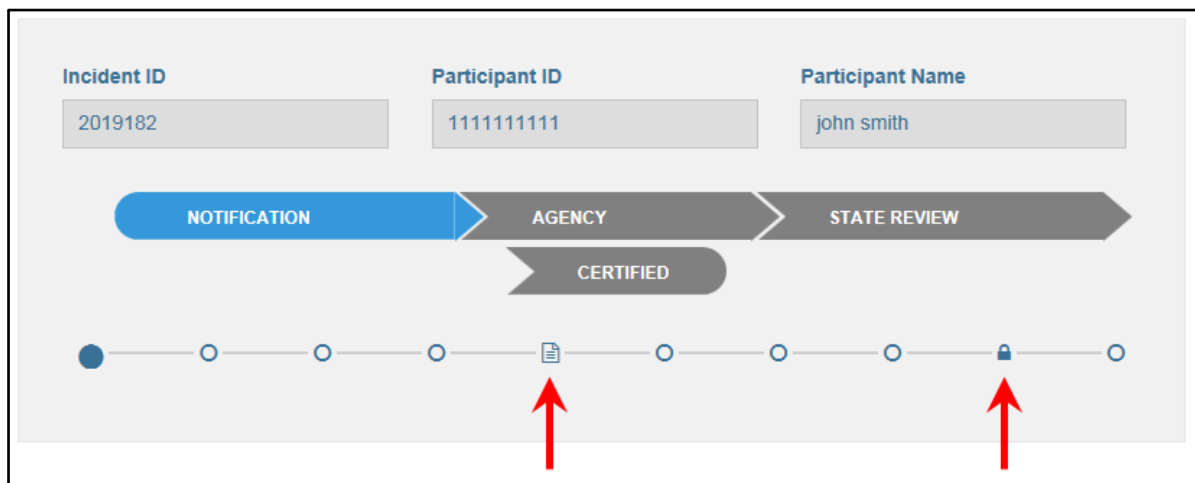


Figure 54 Figure 2 Progress Header

6. In the “Participant Information” section, enter a Participant ID in the *Participant ID* field. All required fields are marked with a red asterisk.

Note: Users are required to perform a search on the participant’s ID before proceeding to the entire incident. If the search finds the participant in the database, the name, gender, and date of birth fields will be prefilled. If the participant’s ID is not found in the database, the user can manually enter the required information.

7. Select **Yes** or **No** to the question regarding whether this is a vulnerable child.
8. Enter the participant’s name in the *First Name*, *Middle Initial/Name*, and *Last Name* fields.
9. Enter the participant’s suffix in the *Suffix* field using the drop-down menu if applicable.
10. Select Male or Female button in the *Gender* field.
11. Enter the participant’s date of birth in the *Date of Birth* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format.
12. Enter the participant’s previous name information in the previous name fields if applicable.
13. Enter the participant’s previous suffix in the *Previous Suffix* field using the drop-down menu if applicable.
14. Select the target group in the *Target Group at the time of incident* field. Target groups are identified as follows:
 - I/DD: Intellectual/Developmental Disability
 - SED: Severe Emotional Disturbance

- PD: Physical Disability

15. Select the program in the *Program* field. Programs are identified as follows:

- CLTS: Children's Long-Term Support Waiver Program
- CCOP: Children's Community Options Program

16. In the "Incident Notification" section, enter the date of the incident in the *Date Incident Occurred* field using the mm-dd-yyyy format or using the calendar by clicking the calendar icon that appears to the right of the date format. This date must be the same as or after the birth date of the participant and cannot be a future date.

17. Select the county in which the incident occurred using the drop-down menu.

18. Select the agency that is responsible for the participant using the drop-down menu.

19. Enter the date the waiver agency was notified of the incident using the mm-dd-yyyy format or using the calendar by clicking the calendar icon that appears to the right of the date format. This date must be the same as or after the incident date and cannot be a future date.

20. Answer the question about who reported the incident to the waiver agency using the drop-down menu.

Note: You can click **Download Incident** on the bottom of the panel to create a PDF of the entire incident. This option is available after the initial save of this screen, which will create the incident.

21. Click **Save & Continue**. A dialog box will appear to confirm you want to leave the page.

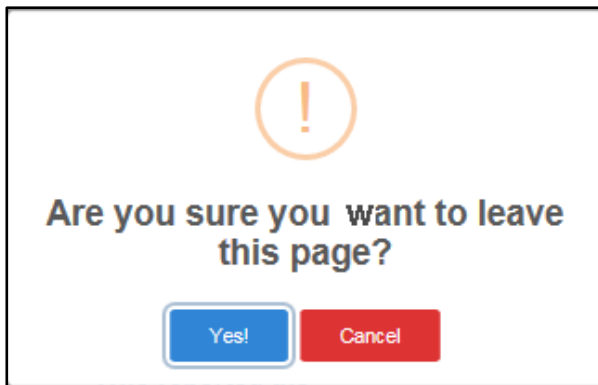


Figure 55 Dialog Box

22. Click **Yes!**

Note: Each time this is clicked, the data the user has entered is saved in the database.

23. The Participant Contact Information panel will be displayed. The participant’s incident ID, ID number, and name information will be prefilled at the top of the panel.

A screenshot of a web application interface. At the top, there are three input fields: "Incident ID" with value "2020670", "Participant ID" with value "1111111111", and "Participant Name" with value "TESTER M TESTED". Below these is a progress bar with four steps: "NOTIFICATION" (active, blue), "AGENCY", "STATE REVIEW", and "CERTIFIED". Underneath the progress bar is a horizontal timeline with several circular markers. The main section is titled "PARTICIPANT CONTACT INFORMATION". It contains several fields: "Primary Phone Number" (value: "XXXXXXXXXX", with a red asterisk and "Phone Number is required" below), "Current Living Arrangement" (value: "'Select'", with a red asterisk and "Living Arrangement is required" below), and "Participant is legally responsible for self?" (checkbox, unchecked). Below this are two sections for "Concerned Entity 1" and "Concerned Entity 2", both labeled "(Parent/Guardian/Representative)". Each section has fields for "First Name", "Middle Initial/Name", "Last Name", "Suffix" (dropdown menu), and "Phone Number" (value: "XXXXXXXXXX"). At the bottom of the form are three buttons: "Previous", "Download Incident", and "Save & Continue".

Figure 56 Participant Contact Information Panel

24. Enter the primary phone number for the child or the child's parent/legal guardian in the *Primary Phone Number* field.
25. Select the current living arrangement from the *Current Living Arrangement* field using the drop-down menu.
26. Check the box if the participant is legally responsible for themselves.
27. Under Concerned Entity 1, enter the parent/guardian/representative's name in the *First Name*, *Middle Initial/Name*, and *Last Name* fields.
28. Enter a suffix in the *Suffix* field if applicable.
29. Enter the parent/guardian/representative's phone number in the *Phone Number* field.
30. If applicable, under Concerned Entity 2, enter the parent/guardian/representative's name in the *First Name*, *Middle Initial/Name*, and *Last Name* fields.
31. Enter a suffix in the *Suffix* field using the drop-down menu if applicable.
32. Enter the parent/guardian/representative's phone number in the *Phone Number* field.
33. Click **Save & Continue**. A dialog box will be displayed to confirm the user wants to leave the page.

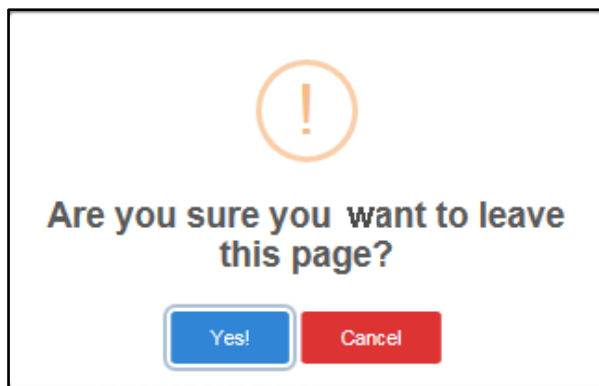


Figure 57 Dialog Box

34. Click **Yes!** The Incident Type, Provider Involvement, Incident Description, and Referral panel will be displayed.

Figure 58 Incident Type, Provider Involvement, Incident Description, and Incident Referral Panel

35. Under the “Incident Type, Type 1” section, select the incident type in the Incident Type field using the drop-down menu. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#).

Note: Selecting the “Other” option from a drop-down menu will bring up a text box description field.

36. Select the incident type detail in the *Incident Type Detail* field using the drop-down menu. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#).

Note: Users can click **Add Incident Type** to add incident types. Up to three incident types can be added. Also, if three incident types are listed and the second incident type is removed, the third incident type would also be removed and would need to be re-entered.

37. Under the “Provider Involvement” section, answer the question asking if the provider was involved with the incident by selecting **Yes, a provider was involved** or **No, a provider was not involved**. If a provider was involved, use the drop-down menu under the *Provider Involvement* field and identify the provider’s agency under *Name of Provider Agency* field.

38. Under the “Incident Description” section, enter where the incident occurred in the *Where did the incident occur?* field using the drop-down menu. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#).

39. Enter a narrative about the incident in the *Incident Description* field. Text is limited to 3,000 characters.

40. Describe what actions were taken to remediate the situation in the *Actions taken to remediate the situation?* field. Text is limited to 3,000 characters.
41. Under the "Incident Referral" section, enter the referred date in the *Referred Date 1* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date.
42. Enter the referral in the *Referred To 1* field using the drop-down menu. Users can enter up to three referrals.
43. Click **Save & Send to DHS**. A dialog box will appear to confirm the user wants to leave the page. The incident status changes to "in progress."

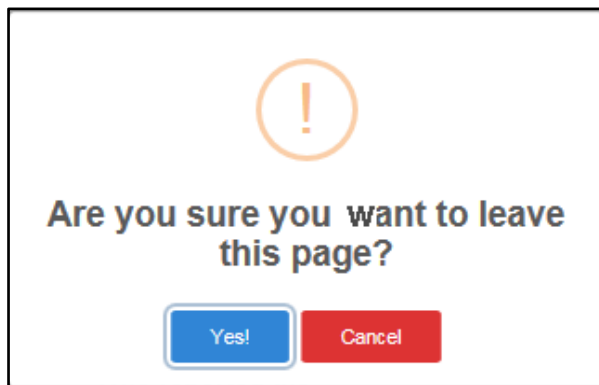


Figure 59 Dialog Box

44. Click **Yes!**
45. An incident notification email will be generated to State administrators and agency staff. The incident notification email includes the following:
 - a. Date the agency was notified
 - b. Incident ID
 - c. Participant ID

d. Submitter Org

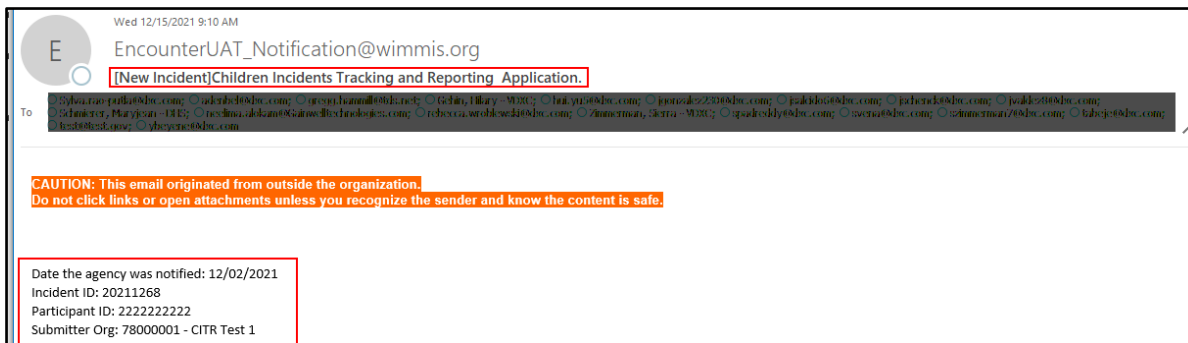


Figure 60 Incident Notification Email

46. The Finalize Initial Save panel will be displayed. The fields under the “Data Entry Worker Credentials” section will be pre-filled based on the login information.

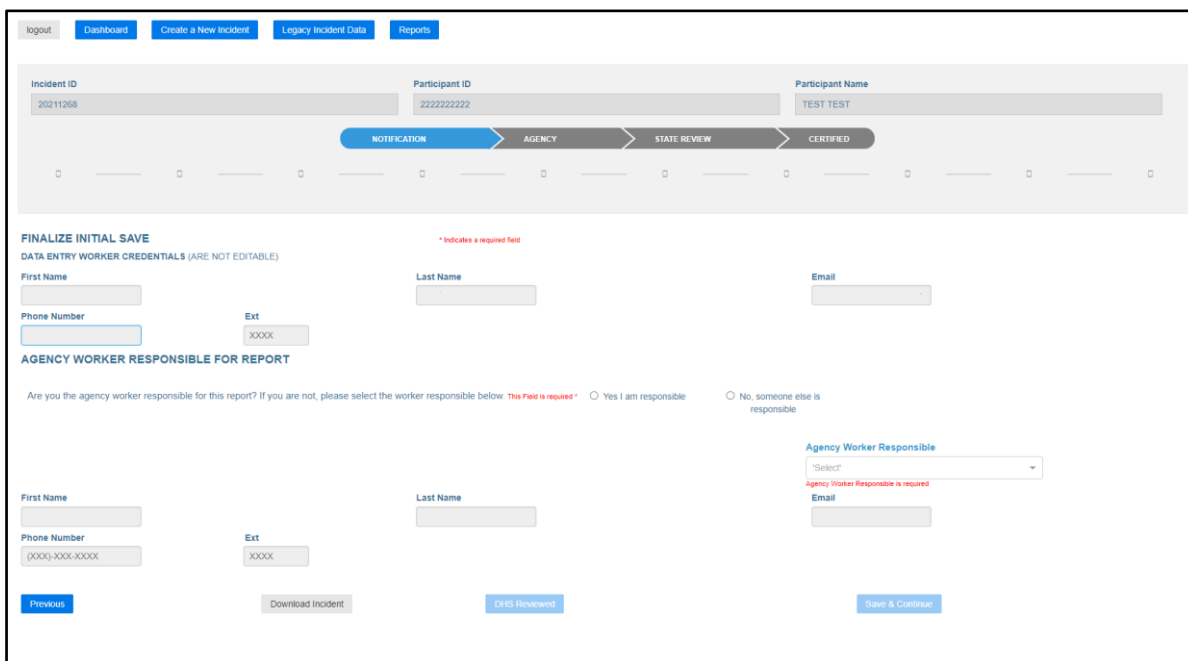


Figure 61 Finalize Initial Save Panel

47. Under the “Agency Worker Responsible for Report” section, select **Yes I am responsible** or **No someone else is responsible** to the question regarding whether the user is the agency worker responsible for this report. If they are not responsible, select the worker who is responsible using the drop-down menu and enter their information in the *First Name, Last Name, Email, Phone Number, and Ext.* fields.

48. Click **Save & Continue**. A dialog box will appear to confirm the user wants to leave the page.

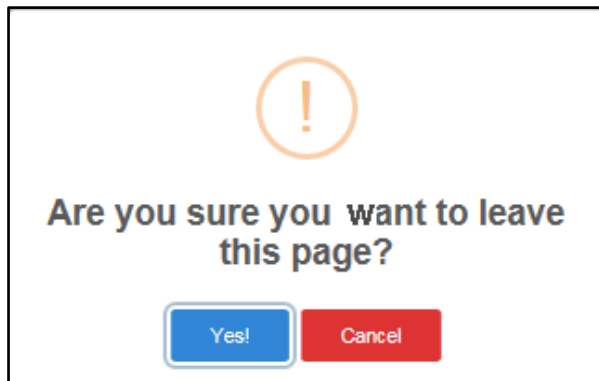


Figure 62 Dialog Box

49. Click **Yes!**

50. The incident moves to the Agency stage and the Alleged Maltreater panel will be displayed.

Figure 63 Alleged Maltreater Panel

51. Under the “Alleged Maltreater, Type 1” section, answer the question asking if the alleged maltreater is known by selecting **Yes, the alleged maltreater is known**; **No, the alleged maltreater is unknown**; or **N/A-there is no alleged maltreater**. If applicable, enter the alleged maltreater’s relationship to the participant using the drop-down menu under the *Relationship to Participant* field and the type of involvement using the drop-down menu under the *Type of Involvement* field.

Note: The user can add an additional maltreater by clicking the **Add Maltreater** box on the far right of the page. Up to three maltreaters can be listed. Also, if three maltreaters are listed and the second maltreater is removed, the third maltreater would also be removed and would need to be re-entered.

52. Under the "Court Order Information" section, answers the question asking if the participant is currently under a court order by selecting **Yes** or **No**. If yes, select the type of court order under the *Type of Court Order* field using the drop-down menu.
53. Under the "Parent/Guardian Notification" section, answer the question asking if the parent/guardian is aware of this incident by selecting **Yes** or **No**. If yes, enter the date the parent/guardian was notified in the *Date parent/guardian was notified* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date.
54. Answer the question asking if the parent/guardian is the subject of the investigation by selecting **Yes** or **No**.
55. Click **Save & Continue**. A dialog box will appear to confirm the user wants to leave the page.

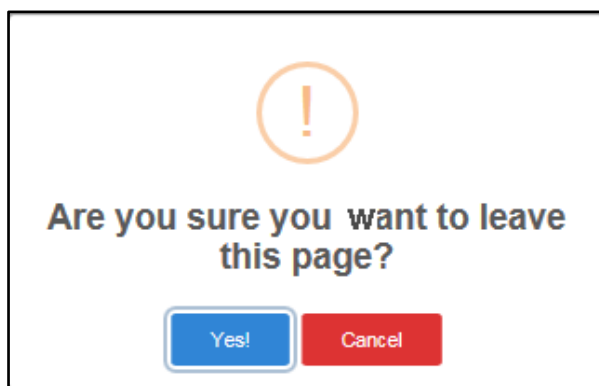


Figure 64 Dialog Box

56. Click **Yes!** The Final Incident Details panel will be displayed.

Figure 65 Final Incident Details Panel

57. Answer the question asking if the participant or their legal representative were informed of the county waiver agency’s (CWA’s) review and response by selecting **Yes** or **No**.

58. Provide information in the following fields:

- Select all persons/agencies contacted by the CWA using the drop-down menu.
- Note any person/entity not notified and why. Text is limited to 3,000 characters.
- Provide details to describe the actions and changes implemented to ensure immediate and ongoing health and safety. Text is limited to 3,000 characters.

59. Answer the question asking if the incident resulted in a substantiated finding of abuse by a government agency using the drop-down menu. If yes, enter the date of substantiation in the *Date of substantiation (Required if answered “Yes”)* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date. If yes, enter the substantiating agencies in the *Substantiating Agencies (Required if answered “Yes”, up to three can be submitted)* field.

60. Answer the question asking if the incident resulted in a substantiated finding of neglect by a government agency using the drop-down menu. If yes, enter the date of substantiation in the *Date of substantiation (Required if answered "Yes")* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date. If yes, enter the substantiating agencies in the *Substantiating Agencies (Required if answered "Yes", up to three can be submitted)* field.
61. Answer the question asking if the incident resulted in a substantiated finding of exploitation by a government agency using the drop-down menu. If yes, enter the date of substantiation in the *Date of substantiation (Required if answered "Yes")* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date. If yes, enter the substantiating agencies in the *Substantiating Agencies (Required if answered "Yes", up to three can be submitted)* field.
62. If pending for sections 59 through 61, the page can be saved without selecting the outcome code.
63. Enter the outcome in the *Outcome* field using the drop-down menu. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#). Note: Outcome options should reflect the result of a Child Protective Services (CPS) investigation.
64. Enter the outcome determination date in the *Outcome Determination Date* field using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date.
65. Enter the remediation action in the *Remediation Action 1* field using the drop-down menu. You can enter up to three remediation actions. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#). Note: A remediation and preventative strategy routinely reflects the results of the CLTS program actions. It may sometimes reflect the results of the CPS program actions.
66. Enter the preventative strategy in the *Preventative Strategy 1* field using the drop-down menu. You can enter up to three preventative strategies. Menu options for this field are available in [Appendix D: Data Fields and Menu Options](#). Note: A remediation and preventative strategy routinely reflects the results of the CLTS program actions. It may sometimes reflect the results of the CPS program actions.

67. Click **Save & Continue**. A dialog box will appear to confirm the user wants to leave the page.

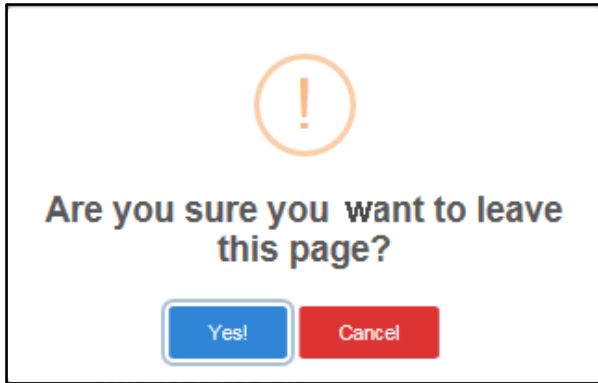


Figure 66 Dialog Box

68. Click **Yes!** The Upload Files and Attached Files panel will be displayed.

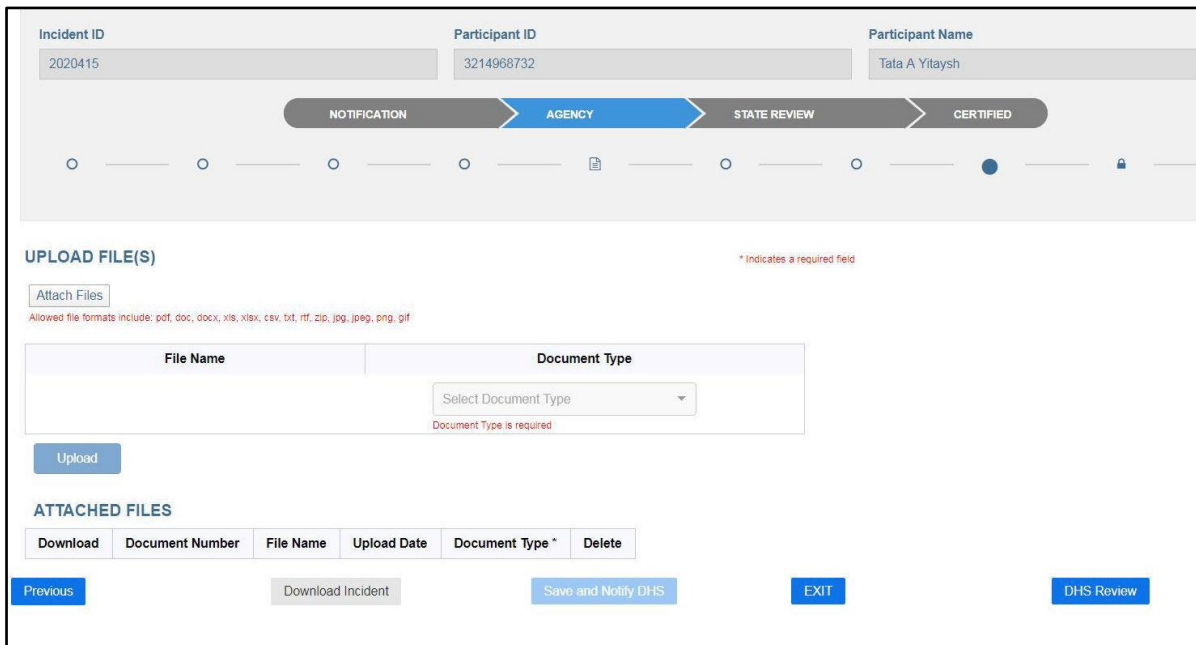


Figure 67 **Figure 3** Upload Files and Attached Files Panel

69. Under the “Upload File(s)” section, click **Attach Files** to attach any additional documents such as a court order, conviction, or provider report. The following file extensions that are allowed for uploading are: .pdf, .doc, .docx, .xls, .xlsx, .csv, .txt, .rft, .zip, .jpg, .jpeg, .png, or .gif.

70. Identify the document type using the Document Type drop-down menu.

71. Click **Upload**. A dialog box will briefly appear and indicate if the document was successfully loaded.

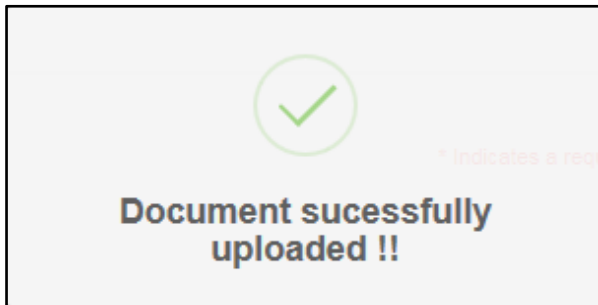


Figure 68 Figure 4 Dialog Box

72. The uploaded file will appear in the “Attached Files” section that displays six columns.

- The *Download* column allows the user to download the file by clicking **Download**.
- The *Document Number* column displays the document number assigned for the file.
- The *File Name* column displays the file name of the uploaded file.
- The *Upload Date* column displays the date the file was uploaded.
- The *Document Type* column displays the document type (for example, court order, provider report).
- The Delete column allows the user to delete the file by clicking **Delete**.

73. When all files have been uploaded, the following options may be available:

- **Save and Notify DHS**—This option will lock the incident for editing and an email will be generated to State and agency staff stating the incident is ready for review. Once DHS completes its review, the agency will receive an email notification.

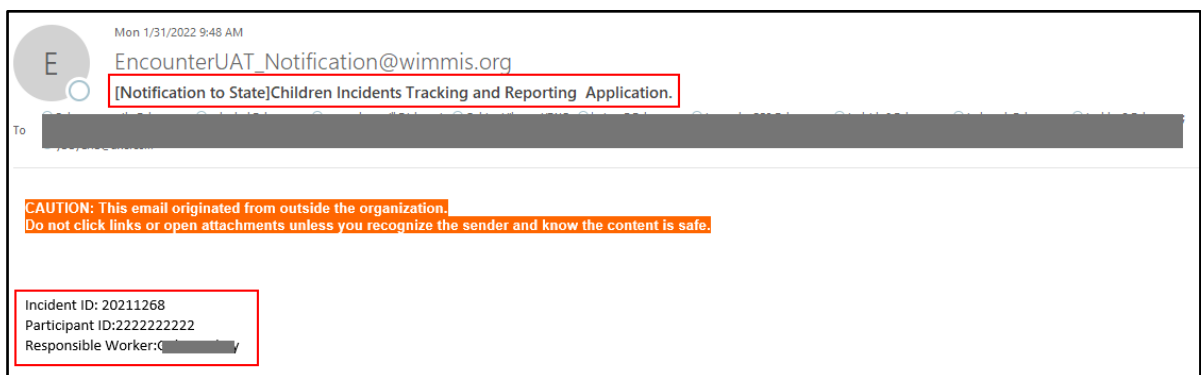


Figure 69 Incident Ready for Review Email



Figure 70 Unlock Email

- **EXIT**—This option will take the user back to the Incidents dashboard.

6 Creating an Incident for an Unlisted Participant

This function allows the user to create a new incident for a participant who may be in the process of being enrolled or transferred to an agency but is not yet listed on the Agency Participants dashboard or for a participant who is only enrolled in the Children's Community Options Program (CCOP) and does not have enrollment in ForwardHealth.

1. Click **Create a New Incident** located on the menu bar of the Incidents or Agency Participants dashboard near the top of the page.

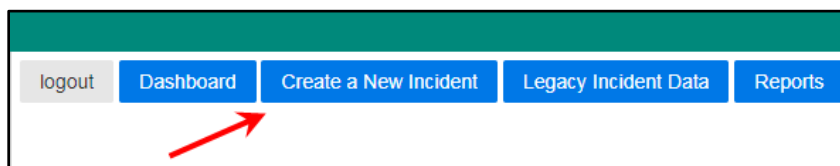


Figure 71 Create a New Incident

2. A dialog box will appear to confirm the user wants to create a new incident.

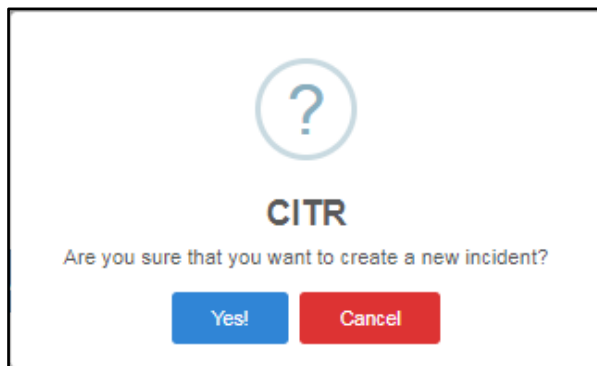


Figure 72 Dialog Box

3. Click **Yes!** Follow the steps in the "Creating an Incident for a Participant Enrolled in CLTS" section beginning with [Step 5](#).

7 Legacy Incident Data

The Legacy Incident Data panel displays the historical data from the manual process that the CITR application is replacing. This data is for historical purposes only and cannot be edited. Legacy data will be included when conducting a search for previous incidents.

1. To view a participant’s legacy incident data, click **Legacy Incident Data** located on the menu bar of the Incidents or Agency Participants dashboard near the top of the page.

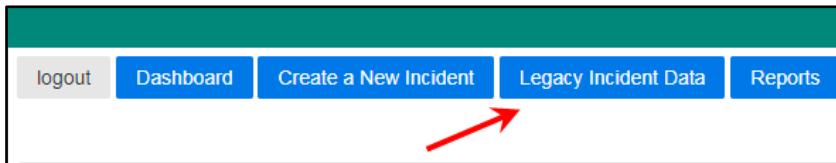


Figure 73 Legacy Incident Data

2. A dialog box will appear to confirm the user’s selection.

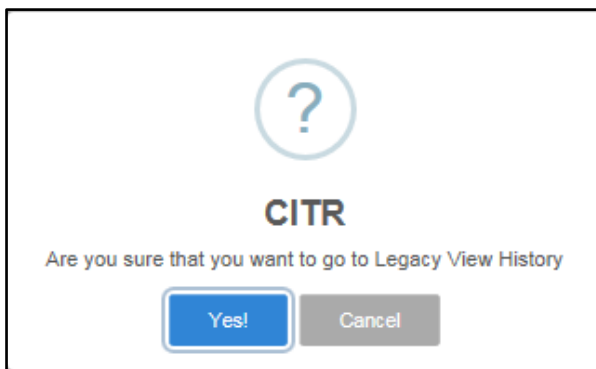


Figure 74 Dialog Box

3. Click **Yes!** Legacy data for each participant will be displayed across nine columns.

Organization ID	Participant ID	Participant Name	Received Date	Report Date	Report Type	Incident Date	Incident Setting	Incident Setting Other
78000001	101010101	Sammy A Sam	2017-12-11 00:00:00.0	2017-11-15 00:00:00.0	1	2017-10-31 00:00:00.0	Child's Home	
78000001	2121212121	Don B Donald	2017-10-12 00:00:00.0	2017-10-10 00:00:00.0	2	2017-10-10 00:00:00.0	Child Care Center	
78000001	6565656565	Kenny C Kendal	2017-12-13 00:00:00.0	2017-09-05 00:00:00.0	3	2017-09-01 00:00:00.0	Community Setting	
78000001	7474747474	Madisonmiddleton Stoughtonveronafitchburg	2017-01-15 00:00:00.0	2017-01-15 00:00:00.0	1	2017-01-15 00:00:00.0	Other	Hospital
78000001	8989898989	Joe D Johnsonsmithski	2017-11-14 00:00:00.0	2017-08-01 00:00:00.0	4	2017-04-06 00:00:00.0	Day Treatment Program	

Showing 1 to 5 of 5 entries Previous 1 Next

Figure 75 Legacy Data Listing

The panel may include the following information:

- The *Organization ID* column displays the identification number of the organization.
- The *Participant ID* column displays the identification number of the participant.
- The *Participant Name* column identifies the participant.
- The *Received Date* column displays the date DHS received the incident report.
- The *Report Date* column displays the date the incident allegation was reported to the CWA.
- The *Report Type* column displays one of the following report types.
 - a. 1 = Original incident report
 - b. 2 = Update to incident report
 - c. 3 = Correction to incident report
 - d. 4 = Incident report closed.
- The *Incident Date* column displays the date the incident occurred.
- The *Incident Setting* column displays the location the incident occurred.
- The *Incident Setting Other* column displays the location the incident occurred if "Other" is selected from the drop-down menu for the incident setting.

Note: The user can search for any of the fields displayed on the panel by populating the **Search** box.

8 Reports

Reports are available to both users and State administrators. Users can run reports only for the organizations they are associated with while State administrators can run reports for all organizations. Multiple organizations can be selected to be included in one report.

1. To view a participant's legacy incident data, click **Reports** located on the menu bar of the Incidents or Agency Participants dashboard near the top of the page.

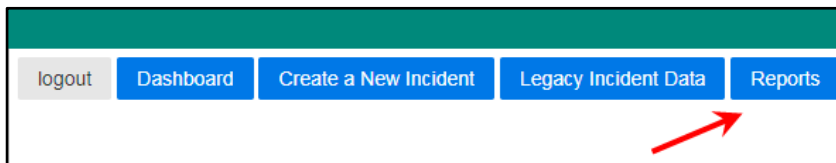


Figure 76 Reports

2. A dialog box will appear to confirm your selection.

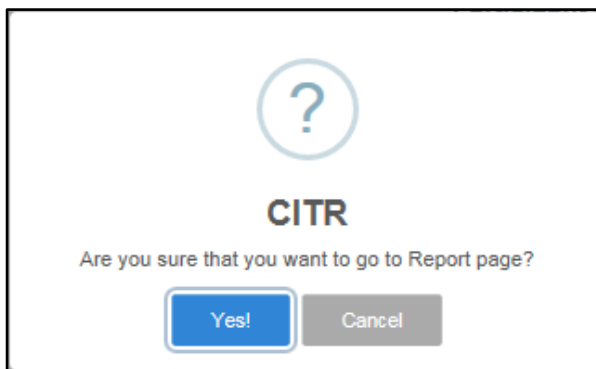


Figure 77 Dialog Box

3. Click **Yes!** The Reports panel will be displayed.

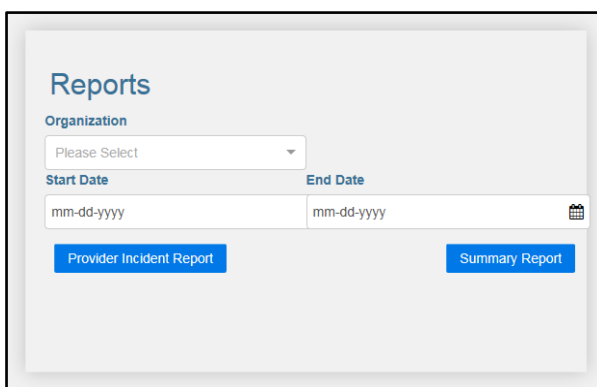


Figure 78 Reports Panel

4. Enter the name of the organization in the *Organization* field using the drop-down menu.
5. Enter the start date in the *Start Date* field using mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date.
6. Enter the end date in the *End Date* field using mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format. This date must be equal to or after the incident date and cannot be a future date.
7. To view the provider incident report, click the **Provider Incident Report**. The file download window will be displayed.

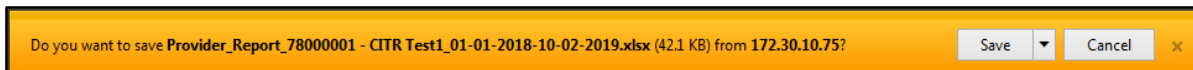


Figure 79 File Download Window

8. Click **Save**. The completed file download window will be displayed.

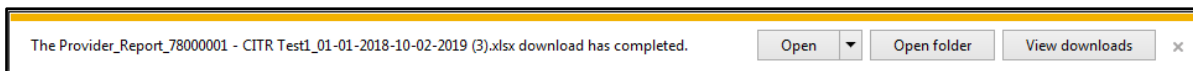


Figure 80 Completed File Download Window

9. Click **Open**. An Excel spreadsheet will be displayed.

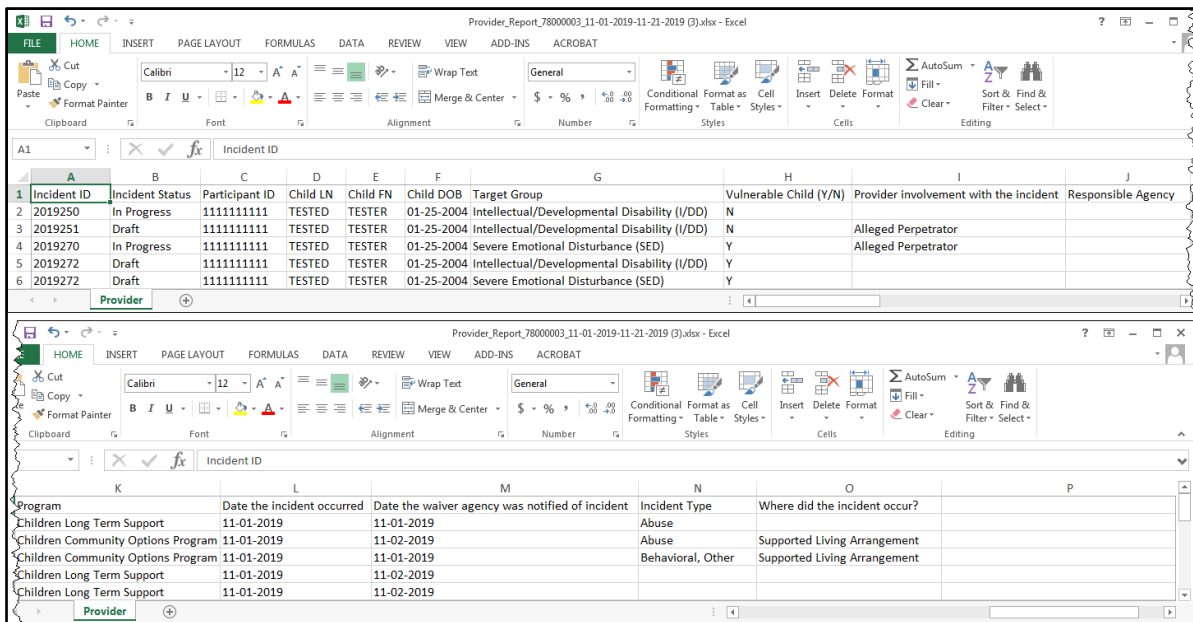


Figure 81 Provider Incident Report

The provider incident report includes the following data elements:

- *Incident ID*—Displays the identification number of the incident.

- *Incident Status*—Displays the status of the incident.
- *Participant ID*—Displays the ID number of the participant.
- *Child LN*—Displays the last name of the participant.
- *Child FN*—Displays the first name of the participant
- *Child DOB*—Displays the date of birth of the participant.
- *Target Group*—Displays one of three target groups the participant is eligible for:
 - a. I/DD: Intellectual/Developmental Disability
 - b. SED: Severe Emotional Disturbance
 - c. PD: Physical Disability
- *Vulnerable Child (Y/N)*—Indicates Y (yes) or N (no) if the participant is a vulnerable child.
- *Provider involvement with the incident*—Identifies the provider’s involvement with the incident.
- *Responsible Agency*—Identifies the responsible agency.
- *Program*—Displays the program that is serving the participant. Programs include the following:
 - a. CLTS: Children’s Long-Term Support Waiver Program
 - b. CCOP: Children’s Community Options Program
- *Date the incident occurred*—Indicates the date the incident occurred.
- *Date the waiver agency was notified of the Incident*—Displays the date the waiver agency was notified of the incident.
- *Incident Type*—Displays the type of incident (for example, abuse, neglect, behavioral, death).
- *Where did the Incident Occur?*—Identifies where the incident occurred.

10. To view the summary report, click the Summary Report. The file download window will be displayed.

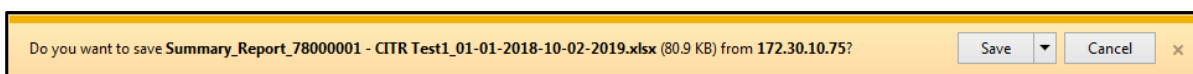


Figure 82 File Download Window

11. Click **Save**. The completed file download window will be displayed.

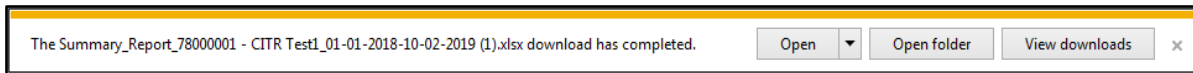


Figure 83 Completed File Download Window

12. Click **Open**. An Excel spreadsheet will be displayed.

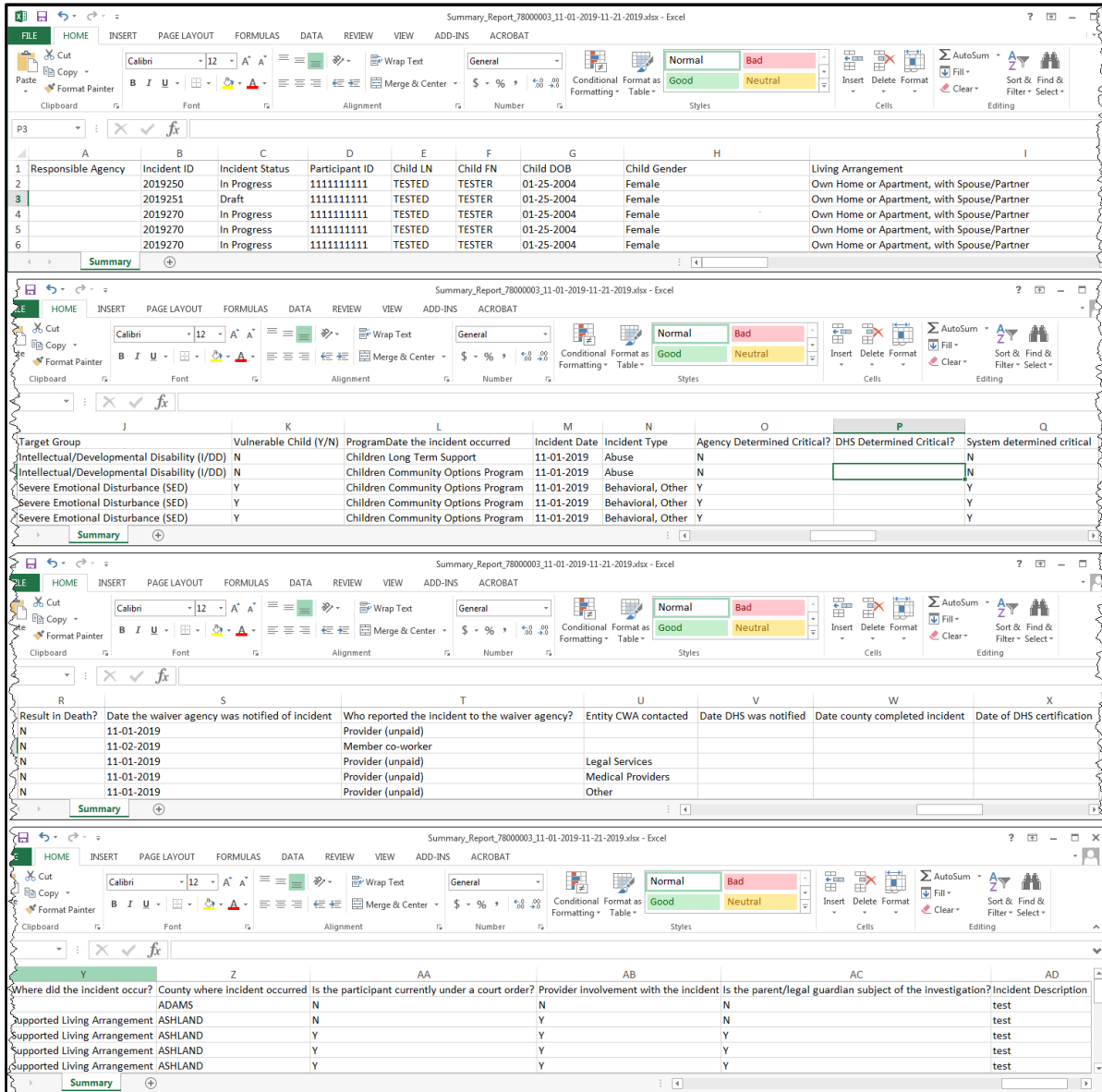


Figure 84 Summary Report

The summary report includes the following data elements:

- *Responsible Agency*—Identifies the responsible agency.

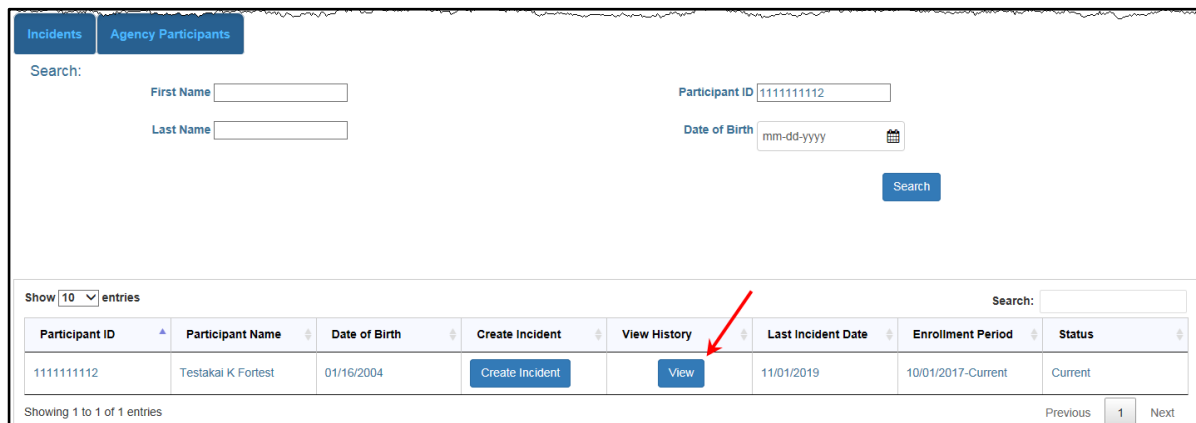
- *Incident ID*—Displays the ID number of the incident.
- *Incident Status*—Displays the status of the incident.
- *Participant ID*—Displays the ID number of the participant.
- *Child LN*—Displays the last name of the participant.
- *Child FN*—Displays the first name of the participant.
- *Child DOB*—Displays the date of birth of the participant.
- *Child Gender*—Displays the gender of the participant.
- *Living Arrangement*—Displays the participant's current living arrangement.
- *Target Group*—Displays one of three target groups the participant is eligible for:
 - a. I/DD: Intellectual/Developmental Disability
 - b. SED: Severe Emotional Disturbance
 - c. PD: Physical Disability
- *Vulnerable Child (Y/N)*—Indicates Y (yes) or N (no) if the participant is a vulnerable child.
- *Program*—Displays the program that is serving the participant. Programs include the following:
 - a. CLTS: Children's Long-Term Support Waiver Program
 - b. CCOP: Children's Community Options Program
- *Incident Date*—Indicates the date the incident occurred.
- *Incident Type*—Displays the type of incident (for example, abuse, neglect, behavioral, death).
- *Date the waiver agency was notified of incident*—Displays the date the waiver agency was notified of the incident.
- *Who reported the incident to the waiver agency?*—Identifies who reported the incident to the waiver agency.
- *Entity CWA contacted*—Identifies the entity the CWA contacted.
- *Date DHS was notified*—Displays the date DHS was notified of the incident.
- *Date county completed incident*—Displays the date the county completed the incident.
- *Date of DHS certification*—Displays the date DHS granted certification.

- *Where did the incident occur?*—Identifies where the incident occurred (for example, family home, school, child care).
- *County where incident occurred*—Displays the county in which the incident occurred.
- *Is the participant currently under a court order?*—Indicates Y (yes) or N (no) if the participant is currently under a court order.
- *Provider involvement with the incident*—Indicates Y (yes) or N (no) if the provider was involved with the incident.
- *Is the parent/legal guardian subject of the investigation?*—Indicates Y (yes) or N (no) if the parent/legal guardian was the subject of the investigation.
- *Incident Description*—Displays a description of the incident.

9 Viewing Incident History

This function allows a user to view the prior history of the participant.

1. On the Agency Participants dashboard, search for an agency participant using the [search function](#). Input any of the following: the participant's first name, last name, ID, and/or date of birth using the mm-dd-yyyy format or use the calendar by clicking the calendar icon that appears to the right of the date format.
2. Click **Search**. Information about the participant will be displayed across eight columns at the bottom of the screen.
3. Click **View** in the View History column for the agency participant.



The screenshot shows the 'Agency Participants' dashboard. At the top, there are tabs for 'Incidents' and 'Agency Participants'. Below the tabs is a search form with fields for 'First Name', 'Last Name', 'Participant ID', and 'Date of Birth'. A 'Search' button is located to the right of the search fields. Below the search form is a table with the following columns: Participant ID, Participant Name, Date of Birth, Create Incident, View History, Last Incident Date, Enrollment Period, and Status. The table contains one entry for Participant ID 111111112, Participant Name Testakai K Fortest, Date of Birth 01/16/2004, Last Incident Date 11/01/2019, Enrollment Period 10/01/2017-Current, and Status Current. A red arrow points to the 'View' button in the 'View History' column of the table. The table also includes a 'Showing 1 to 1 of 1 entries' indicator and 'Previous', '1', and 'Next' navigation buttons.

Figure 85 View History

4. The [Participant Incident History](#) panel will be displayed.

10 Editing an Incident

This function allows the user to edit an existing incident for an agency participant. Note: Incidents in “DHS Review” or “Certified” status cannot be edited and must be unlocked.

1. On the Incidents dashboard, click the Incident ID number in the Incident ID column for the agency participant.

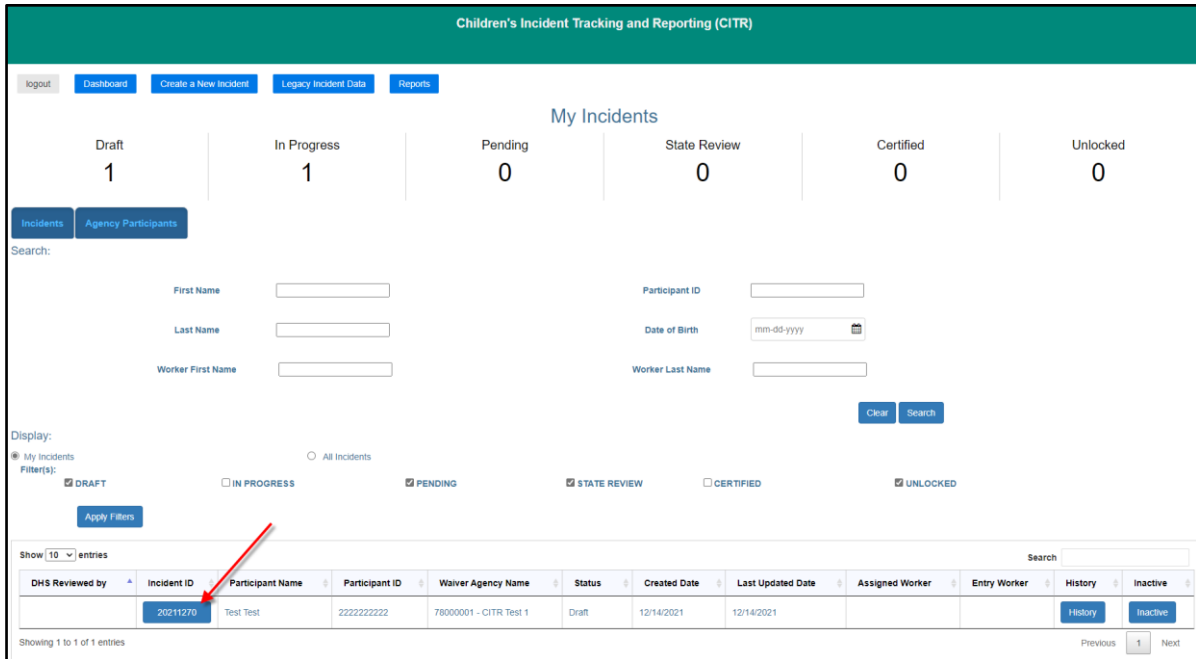


Figure 86 Edit Incident

2. A dialog box will appear to confirm the user’s selection.

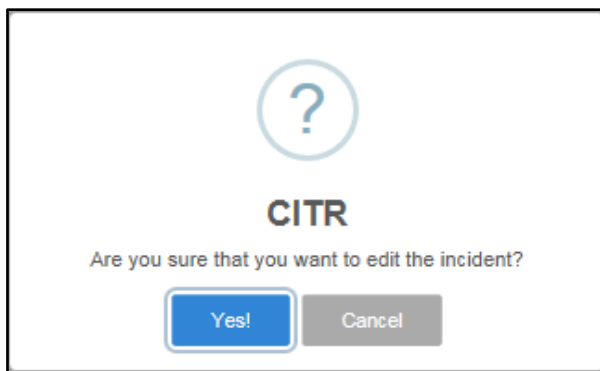


Figure 87 Dialog Box

3. Click **Yes!** The user will be able to access and edit all the panels associated with the incident.

11 Appendix A: Security Roles and Allowable Functions

	State Super User	State Program User	State Regional User	Security Officer Waiver Agency	Waiver Agency Administrator	Waiver Agency Level 1	Waiver Agency Level 2
All Access	X						
View Records	X	Statewide	Assigned specific organizations for email notifications Statewide	Agency Specific	Agency Specific	Agency Specific	Agency Specific
Edit	X				X	X	X
Add New Records	X				X	X	X
Delete Records	X				X	X	
Certify Data-Final State	X	X	X				
Unlock a Closed Incident	X	X	X				
Password Administration	X			X			
Add a New User	X			X			
Inactivate a User	X			X			
Send for State review	X				X	X	
Upload File to Incident	X				X	X	X

	State Super User	State Program User	State Regional User	Security Officer Waiver Agency	Waiver Agency Administrator	Waiver Agency Level 1	Waiver Agency Level 2
Reports	Statewide	Statewide	Statewide	Agency Specific	Agency Specific	Agency Specific	Agency Specific
Inactivate an incident	X	X	X	X	X	X	X

Specific notes and responsibilities for certain security roles include the following:

- Only the State Regional User should receive notification emails only for incidents from their assigned agencies.
- The State Program User role should allow Bureau of Children’s Services staff to view all incident reports in the state without receiving notification emails.
- The Bureau of Children’s Services may designate a staff person(s) to be assigned the State Super User role that is responsible for granting and modifying state user roles, assigning agencies, and deleting access.
- The State Super User or the help desk is able to deactivate a Regional User and set up a new one. They are also able to modify the permissions and organizations within the region.
- A Waiver Agency user may deactivate incidents for which they are the responsible worker.

12 Appendix B: Supported Web Browsers

When the user launches the CITR application, it is presented through their [web browser](#) on a Microsoft Windows, Apple macOS, or Apple iPad computing platform. The supported web browsers are listed in the following table. The left column identifies the computing platform with the web browser name and the versions supported across the row.

If the user is not familiar with the computing platform and web browser they are using, they should contact their local county IT staff for assistance. The user can contact the [Helpdesk to support CITR users](#) if their local IT technical resource is not able to support their request.

Example: If a user uses a Windows platform running the Chrome web browser, the Help=>About Google Chrome menu in the Chrome web browser control panel needs to state version number 79 or back level. If it is higher than version 79, it should still work as it is a "back level" supported application.

If the user is using a web browser that does not have *back level* support listed, they should consider moving to one of the web browsers that does, which are listed in blue in the following table.

Supported Web Browsers for the Children’s Incident Tracking Report Application							
Platform	Operating System Version	Web Browser					
		Edge	Firefox	Chrome	Opera	Yandex	Safari
Windows	7, 8, 8.2, 10 and XP	V 79 and XP not supported	V72 and back level*	V79 and back level*	V67 and back level*	V14.12	Not Supported
macOS	Catalina Mojave High Sierra Mavericks Sierra Yosemite El Capitan	V79	V72 and back level*	V72 and back level*	V67 and back level*	V14.12 Not available on Catalina release	V13 and back level*
iPad	iPad Pro 12.9 2018 V 12 iPad Pro 12.9 2018 V 13 iPad Pro 11 2018 V 12 iPad Pro 12.9 2017 V 11 iPad Pro 9.7 2018 V 11						
<p>All mobile phones are not supported.</p> <ul style="list-style-type: none"> • iPhone Operating System (iOS) not supported. • Android Operating System not supported. 							

* Web browser versions that are still available prior (back level) to the version listed are supported.

13 Appendix C: Support Resources

If the user has questions or need assistance, the following resources are available:

- Phone: Helpdesk to support CITR users—608-224-6007 (Available Monday through Friday from 8 a.m.–4:30 p.m. Closed on weekends and holidays.)
- Email address: VEDSLTCIESHelp@wisconsin.gov
- CWA CLTS supervisor/lead—Is the contact for approving and submitting user access requests. The CWA CLTS supervisor/lead is required to submit the [Encounter New User Request form](#), F-21334, to the helpdesk in order to grant access for new users to the CITR application.

Please be prepared to supply the following:

- Personal contact information to confirm identity including name, employee ID, work location, and phone number
- A brief description of the issue
- When the issue needs to be resolved

14 Appendix D: Data Fields and Menu Options

Data fields and the available drop-down menu options for each field are listed below:

14.1 [Incident Type](#)

- 01—Abuse
- 03—Death
- 07—Exploitation
- 05—Hospitalization
- 04—Law Enforcement
- 06—Neglect
- 08—Unapproved use of Restrictive Measures
- 99—Other

14.2 [Incident Type Detail](#)

- 01—Abuse—Emotional or psychological
- 03—Abuse—Physical
- 04—Abuse—Sexual or exploitation
- 07—Abuse—Verbal
- 12—Death—Anticipated
- 11—Death—Other
- 15—Death—Suicide
- 16—Death—Unexplained
- 18—Exploitation—Financial misappropriation of the participant's funds or property
- 40—Hospitalization—Error in medical or medication management that result in a significant adverse reaction
- 42—Hospitalization—Psychiatric: Private facility

- 41—Hospitalization—Psychiatric: State facility
- 44—Law enforcement—Contact
- 38—Law enforcement—Contact: Behavioral emergency
- 39—Law enforcement—Investigation
- 20—Law enforcement—Investigation: Alleged perpetrator
- 22—Law enforcement—Investigation: Alleged victim
- 43—Neglect—Dangerous living situation
- 30—Neglect—Lack of food/nutrition
- 32—Neglect—Lack of supervision
- 29—Neglect—Medical/Failure to seek medical attention
- 37—Unapproved use of Restrictive Measures—Misuse of mechanical restraint or protective equipment
- 46—Unapproved use of Restrictive Measures—Use of isolation or seclusion
- 45—Unapproved use of Restrictive Measures—Use of manual restraint
- 99—Other

14.3 Where did the incident occur?

- 07—Adult Family Home
- 34—Child care
- 14—Children's Group Home
- 18—Community setting
- 08—Foster Home
- 11—Own Home/Apartment
- 19—Residential setting (not participant's home)
- 21—Respite setting
- 25—School
- 31—Transporting of participant
- 98—Unknown

- 99—Other

14.4 Outcome

- 01—Abuse—Citation
- 02—Abuse—Criminal conviction
- 03—Abuse—Other
- 04—Abuse—Substantiated by a government agency
- 05—Abuse—Unable to substantiate
- 06—Abuse—Unsubstantiated by a government agency
- 07—Death—Abuse
- 08—Death—Accident
- 14—Death—Neglect
- 15—Death—Other
- 19—Death—Suicide
- 20—Death—Unexplained
- 40—Exploitation—Substantiated by a government agency
- 41—Exploitation—Unable to substantiate
- 42—Exploitation—Unsubstantiated by a government agency
- 21—Hospital—Hospitalization due to involuntary psychiatric emergency
- 22—Hospital—Hospitalization due to urgent medical emergency
- 23—Hospital—Hospitalization due to voluntary psychiatric emergency
- 26—Law enforcement—Other or unknown
- 27—Law enforcement—Participant committed a crime
- 28—Law enforcement—Participant did present a safety risk to self or others
- 30—Law enforcement—Participant was the victim of a crime
- 32—Medication error
- 35—Missing person—Participant or caregiver located after unanticipated absence
- 36—Missing person—Participant or caregiver still missing after unanticipated absence

- 29—Neglect—Citation
- 33—Neglect—Criminal conviction
- 34—Neglect—Other
- 37—Neglect—Substantiated by a government agency
- 38—Neglect—Unable to substantiate
- 39—Neglect—Unsubstantiated by a government agency
- 43—Out of home placement
- 99—Other

14.5 Remediation Action 1

- 02—Change personnel working with the participant
- 03—Change provider agency
- 04—Court order (participant)
- 05—Court order (provider)
- 06—Criminal conviction (participant)
- 07—Criminal conviction (provider)
- 08—Emergency detention
- 09—Increase external monitoring (for example, CPS, APS)
- 10—Mental health inpatient admission
- 23—No remediation action
- 11—Participant was or will be relocated to another setting
- 14—Provider education on appropriate use of emergency restrictive measures
- 15—Provider license revoked
- 16—Provider training
- 17—Referral to Disability Rights Wisconsin
- 18—Referral to district attorney/law enforcement agency
- 19—Report to CPS or APS
- 20—Report/Refer to caregivers

- 21—Terminate service
- 22—Terminate staff
- 99—Other

14.6 Preventative Strategy 1

- 01—Add new support or service
- 23—Add or change backup/crisis plan
- 02—Behavior intervention plan, initiate or modify
- 03—Behavioral consult
- 04—Change provider staff serving the participant
- 05—Dietary change(s)/modification(s)
- 06—Environmental modification
- 07—Extension of treatment or supervision
- 10—In-Home support, initiate or increase
- 08—Increase supervision of participant
- 09—Individualized Education Plan review
- 11—Medically related consult
- 12—Medication review and/or adjustment
- 13—Modify Individual Service Plan
- 22—No preventative strategy
- 14—Participant education about boundaries, safe decision-making, and risks
- 15—Provider training or retraining
- 16—Referral for a new support or service
- 17—Referral, psychiatric
- 18—Restrictive measures application, initiate
- 19—Support and Service Coordinator and/or service team makes more frequent contact with participant/provider
- 20—Team meeting to discuss prevention plan with provider(s)/participant/guardian/family and confirm the prevention and remediation actions each member will implement

- 21—Terminate service
- 99—Other

12 Appendix E: Glossary

Children's Long-Term Support Waiver Program (CLTS): The CLTS Waiver Program is a Home and Community-Based Service (HCBS) Waiver that provides Medicaid funding for children who have substantial limitations in their daily activities and need support to remain in their home or community.

Children's Community Options Program (CCOP): The CCOP provides supports and services to children living at home or in the community who have one or more of the following long-term disabilities – developmental disabilities, physical disabilities, and/or severe emotional disturbances.

Participant ID: This ID is the ForwardHealth Participant ID or Master Client Index (MCI) ID.

Vulnerable Child: A vulnerable child is a child who is either eligible for more than one of the three target groups served by the CLTS programs (intellectual/developmental disability, physical disability, or severe emotional disturbance), as determined by the Children's Long Term Support Functional Screen (CLTS FS), or has a high level of life-sustaining needs (nutrition, fluids, or medical treatment) with a limited informal support network. In addition, at least one of the following must apply:

- The child is isolated with limited or no adult contact outside the home and is not available to be observed.
- The child is nonverbal and unable to communicate.
- The child is medically complex, requires significant care from a caregiver or parent, and is highly dependent on others to meet basic needs.
- The child is the subject of current or historical child abuse and neglect reports.
- The child has a primary caregiver who is actively abusing substances.
- The child is dependent on caregivers or parents with limited cognitive, emotional, and/or behavioral capacity to provide for these needs.

Incident Review Statuses:

- **Draft**—This status indicates the incident report is still being drafted.
- **In Progress**—This status indicates initial notification to DHS has been made but the waiver agency has not completed the report. The status is changed from "Draft" to "In Progress" when the user selects "Save & Send to DHS" on the [Finalize Initial Save panel](#).
- **Pending**—If any one of the following substantiation questions from the [Final Incident Details panel](#) are answered as "Pending," the incident status will indicate the report is pending at the final submission to DHS. When all the questions are answered with a "Yes"

or "No" response, the incident will have a status of either "Certified" or "State Review" when it is submitted to DHS:

- a. Did this incident result in a substantiated finding of abuse by a government agency?
- b. Did this incident result in a substantiated finding of neglect by a government agency?
- c. Did this incident result in a substantiated finding of exploitation by a government agency?

Note: When an incident has been in the status of pending for 60 days, an email will be sent warning that the user is approaching the 90-day limit and reminding them to update the incident report. Another email will be sent when an incident has been in a status of pending for 90 days and they will be reminded to update the incident report.

- State Review—This status indicates the incident report has been completed by the waiver agency and DHS is reviewing.
- Certified—This status indicates that DHS has completed review and the incident report is complete.
- Unlocked—This status indicates the State administrator has unlocked the incident report to allow the user to edit the incident after it has been sent to DHS. This is usually done when DHS requires additional information.