Critical Incident Reporting System

Agency User Guide

Introduction

The EOEA Critical Incident Report (CIR) System provides agencies with a method for reporting the specifics of a critical incidents as required per programmatic instructions involving a Home Care–enrolled consumers, Protective Services–involved consumers and/or consumers living in Congregate or Supportive housing. EOEA evaluates the need to report the incident to the Executive Office of Health and Human Services (EOHHS), depending on the nature and severity of the incident.

In addition, EOEA tracks critical incident report data to ensure that all ASAP staff and contracted providers take action to reduce and/or prevent harm to elders served by ASAPs, their workforce members, and caregivers/contracted providers. EOEA also ensures that all involved in the care of elders promptly report and take corrective action in response to incidents impacting the health and welfare of consumers.

A ***reportable critical incident*** is any sudden or progressive event that requires immediate attention and action to prevent/minimize a negative impact on the health and welfare of any consumer(s) served by an agency.

Follow established guidelines regarding what constitutes a critical incident and the required timeframe for reporting incidents. The new electronic CIR system is simply a change to the method of transmission and review of critical incident reports.

Contents

First Login

Step-By-Step Instructions to Configure Your Account and Launch CIR

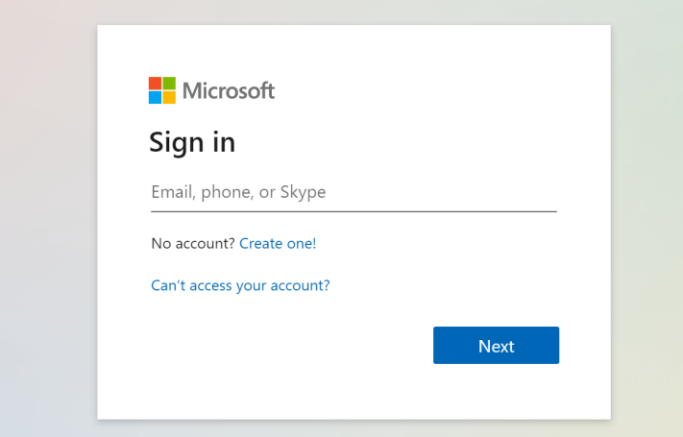
NOTE FOR USERS WHO ACCESS OTHER MICROSOFT ENVIRONMENTS

*The new environment for **Critical Incident Reporting** and other UMass-hosted applications is a Microsoft-hosted environment. Some users – but not all -- may also be using Microsoft-hosted environments to run other applications, which may include Microsoft Office 365 applications like email.*

*If this is the case for you, we recommend that you attempt to access each of your Microsoft environments via a separate web browser (for example, make connections to Critical Incident Reporting from a Chrome browser, and make connections to Microsoft email from an Edge browser). **We recommend Chrome and Firefox as browsers for accessing UMass applications.** Another approach would be to completely log out from one Microsoft environment before launching a connection to the new environment for UMass-hosted applications. Step 3 below contains additional information on Microsoft connections.*

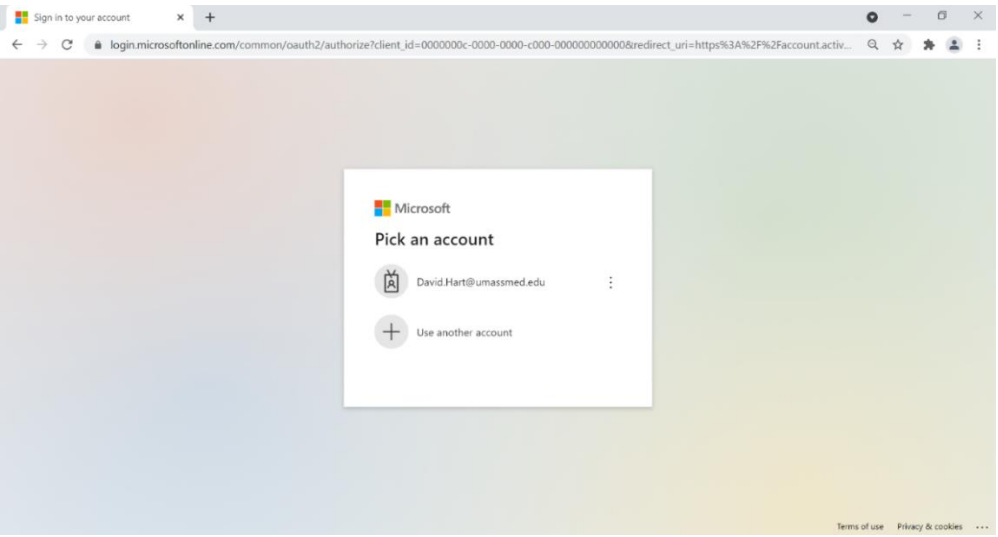
1. Access https://myapps.microsoft.com from your web browser (Chrome or Firefox recommended).

2. Next, a Microsoft log in page with title “Sign In” is displayed. Enter your User ID as it appears in the “User ID” field of the email you received with Subject line **Your new EOEA Online Account for Critical Incident Reporting**.

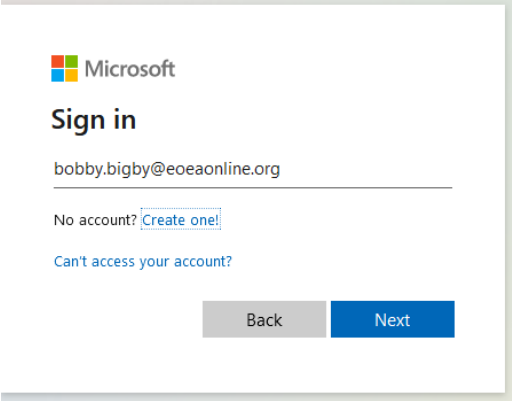


3. If you have previously accessed other Microsoft environments from the same browser on the same computer, you may automatically be logged into an account from a different Microsoft environment, or, you may see "Pick an Account" with account names associated with your previous activity (see screen image below). If you are logged into a different Microsoft environment, please launch another browser application (Chrome and Firefox are recommended) to initiate your connection to Critical Incident Reporting via https://myapps.microsoft.com.

   If you don't see an account that looks like your *firstname.lastname* followed by *@eoeaonline.org*, (e.g., robert.young@eoeaonline.org), click the plus sign (+) adjacent to "Use another account" (see screen image below).

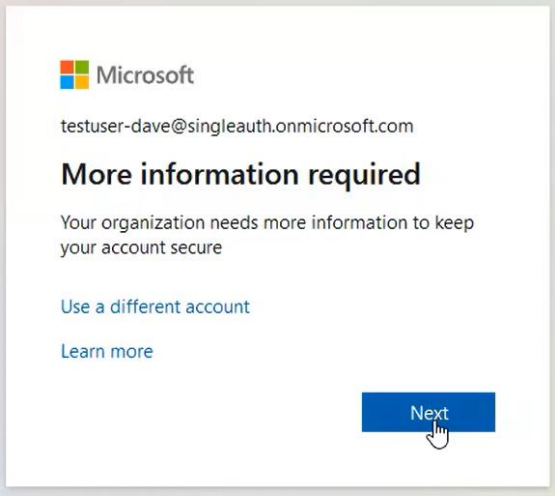


4. If you clicked the **+** next to "Use another account", a Sign in prompt will be displayed as shown here:

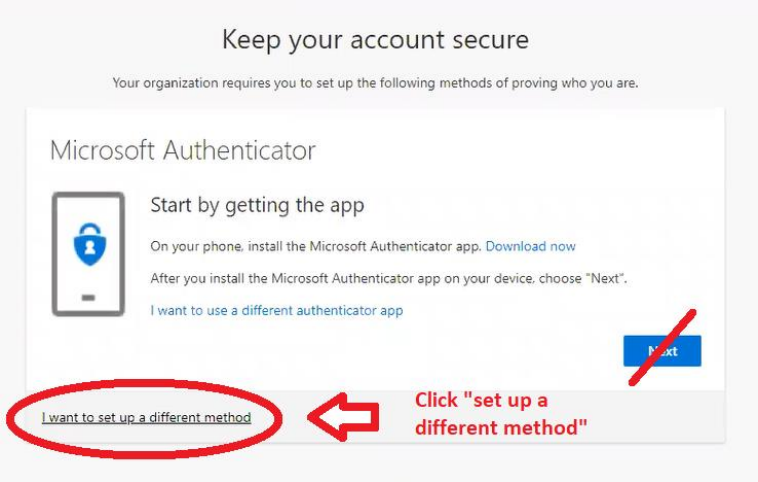


After specifying your username,
click **Next** and you'll be prompted for your password.

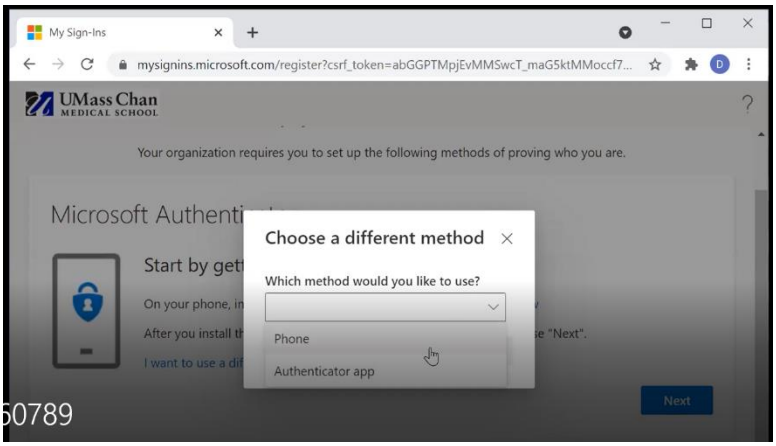
5. Next, you will be guided through a sequence of screens in which you will configure your account and security settings. The first of these screens is shown on the next page. Click **Next** in this screen.



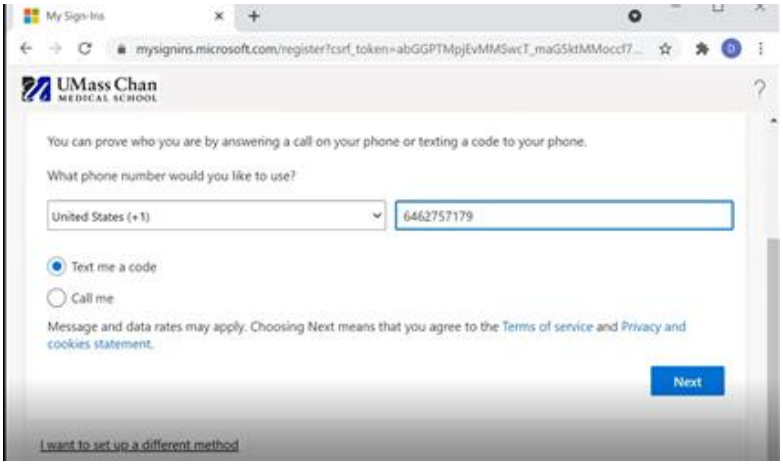
6. Next, the system will guide you through steps to configure security functionality in the new environment. The first of these configuration screens is displayed below. **Select "I want to set up a different method" annotated in red below** (rather than the default option, Microsoft Authenticator).



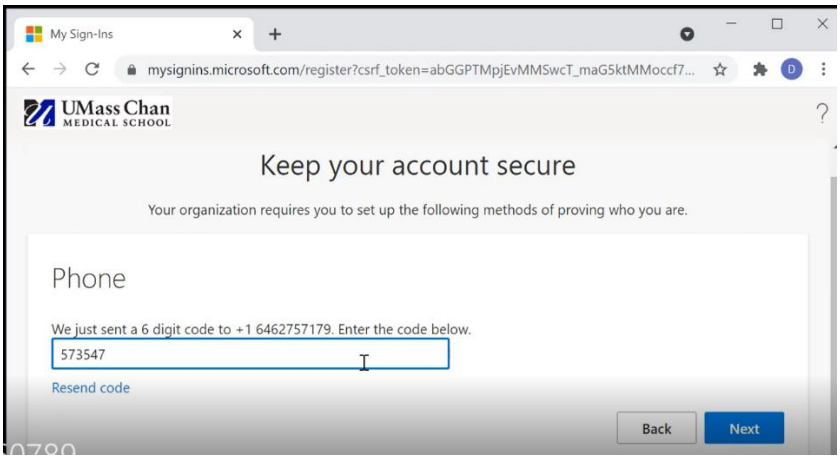
7. After you click to use another method, a dropdown displays, showing the available methods (see screen image below). Select **Phone** from the dropdown, then click the Confirm button.



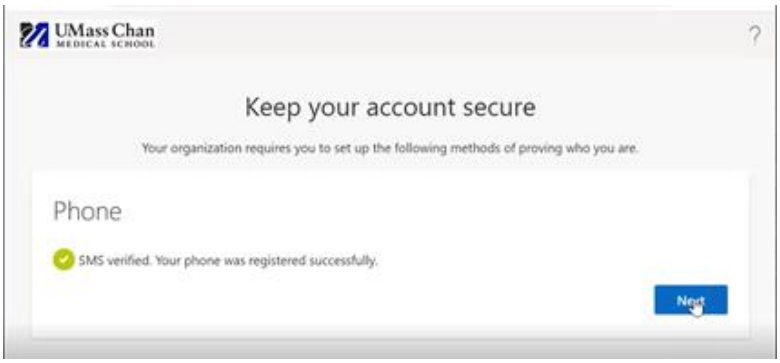
8. Next, a screen displays for you to configure the phone number which would receive a call or text message when you have forgotten your password and need to reset it. You may configure either to receive a text message or a phone call as part of the reset process. The screen image on the next page shows the scenario where the user wants to receive a text message. After you provide your phone number and select Text or Call, press Next.



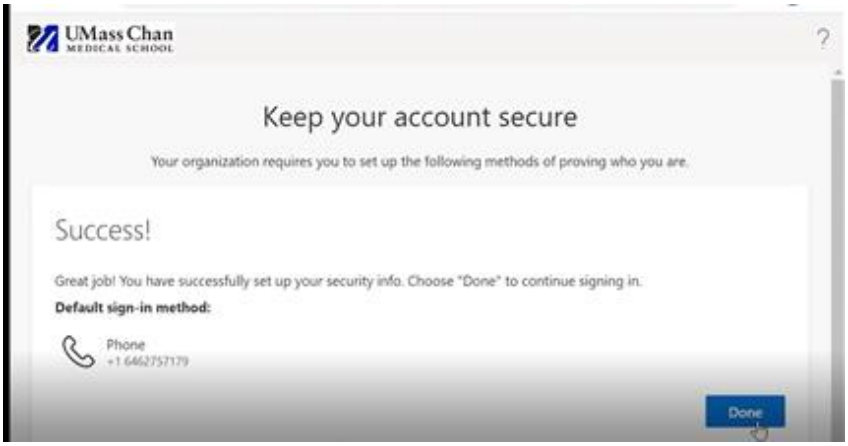
9. After pressing "Next", you will receive either a phone call or text message, depending on your selection. In the case of a text, enter the six-digit code from the text message (see screen image below). In the case of a phone call, respond to the prompt in the call. Then, press **Next**.



Next, a status screen displays (image below), indicating you have successfully registered your Phone security method, which will be used to confirm your identity when you click "I forgot my password" in future sessions. Press **Next** on this screen.

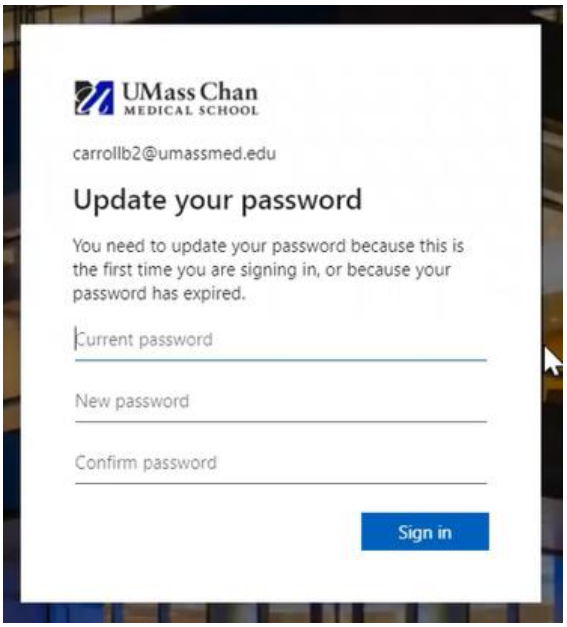


10. An additional screen displays, confirming the successful setup of your account's security information. Click **Done** on this screen.

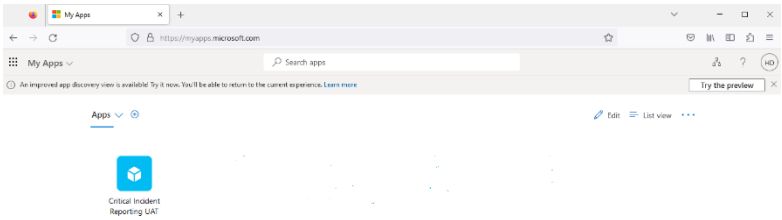


11. Next, you will be prompted to specify a permanent password (see screen image below). The requirements for a permanent password are:

    - At least 8 characters
    - Must contain 3 of the following: Uppercase character, lowercase character, number, special character (*#@$%^&!)
    - Permanent passwords are valid for 60 days, after which you'll be prompted to create a new password.



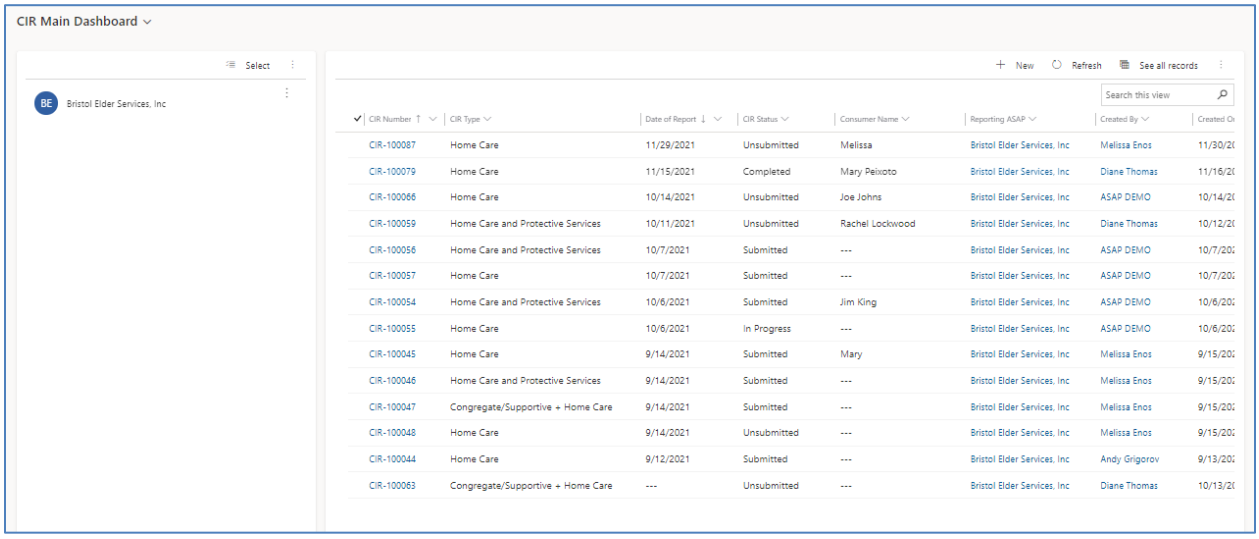
Next, your Myapps landing page (image below) displays an icon for each application to which you have access. Initially, you have access to **Critical Incident Reporting** as depicted below. As we deploy more UMass-hosted applications to the new environment, other icons may also display.



1. Upon your first successful login, you will be prompted by the system to review and agree to a *Data Use Agreement* from UMass. This is only required for your first login. (see Appendix B)

The CIR System Dashboard

After logging in, you will see the CIR system dashboard, image below. The name of your agency will appear on the left, and a list of previous incident reports involving your agency (if applicable) appear on the right.



CIR Number	CIR Type	Date of Report	CIR Status	Consumer Name	Reporting ASAP	Created By	Created On
CIR-100087	Home Care	11/29/2021	Unsubmitted	Melissa	Bristol Elder Services, Inc	Melissa Enos	11/30/20
CIR-100079	Home Care	11/15/2021	Completed	Mary Peixoto	Bristol Elder Services, Inc	Diane Thomas	11/16/20
CIR-100066	Home Care	10/14/2021	Unsubmitted	Joe Johns	Bristol Elder Services, Inc	ASAP DEMO	10/14/20
CIR-100059	Home Care and Protective Services	10/11/2021	Unsubmitted	Rachel Lockwood	Bristol Elder Services, Inc	Diane Thomas	10/12/20
CIR-100056	Home Care and Protective Services	10/7/2021	Submitted	---	Bristol Elder Services, Inc	ASAP DEMO	10/7/202
CIR-100057	Home Care	10/7/2021	Submitted	---	Bristol Elder Services, Inc	ASAP DEMO	10/7/202
CIR-100054	Home Care and Protective Services	10/6/2021	Submitted	Jim King	Bristol Elder Services, Inc	ASAP DEMO	10/6/202
CIR-100055	Home Care	10/6/2021	In Progress	---	Bristol Elder Services, Inc	ASAP DEMO	10/6/202
CIR-100045	Home Care	9/14/2021	Submitted	Mary	Bristol Elder Services, Inc	Melissa Enos	9/15/202
CIR-100046	Home Care and Protective Services	9/14/2021	Submitted	---	Bristol Elder Services, Inc	Melissa Enos	9/15/202
CIR-100047	Congregate/Supportive + Home Care	9/14/2021	Submitted	---	Bristol Elder Services, Inc	Melissa Enos	9/15/202
CIR-100048	Home Care	9/14/2021	Unsubmitted	---	Bristol Elder Services, Inc	Melissa Enos	9/15/202
CIR-100044	Home Care	9/12/2021	Submitted	---	Bristol Elder Services, Inc	Andy Grigorov	9/13/202
CIR-100063	Congregate/Supportive + Home Care	---	Unsubmitted	---	Bristol Elder Services, Inc	Diane Thomas	10/13/20

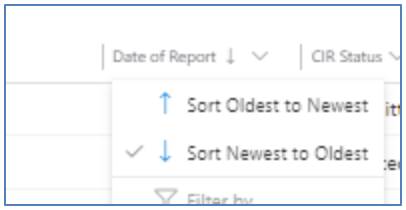
The Incident Reports you are allowed to view are determined by your user role. In the example above, the user has the Home Care user role, so they can only see Incident Reports that involve Home Care. The same holds true, respectively, for Protective Services and Housing agency users.

Your list of Incident Reports includes the following information for each Incident Report:

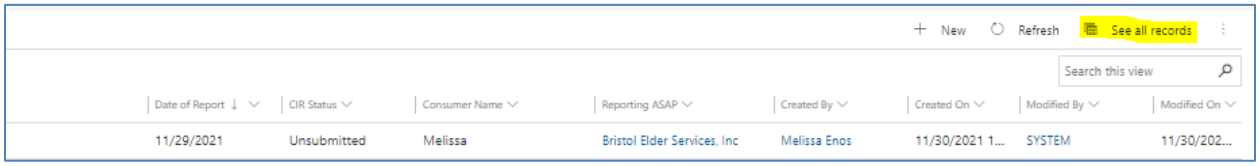
- **CIR Number** – a system assigned, unique ID
- **CIR Type** – displays the department(s) involved in creating/reviewing an incident. More information on report types can be found in the Submitting a Critical Incident Report section below.
- **Date of Report** – IR creation date
- **CIR status** – Unsubmitted/Submitted/In Progress/Completed
- **Consumer Name**
- **Reporting ASAP**
- **Created by**
- **Created on**
- **Modified by**
- **Modified on**

You can **sort** and **filter** your Incident Report list in multiple ways.

To **sort** by a selected column, click the down arrow at the top of the column and choose desired sort.

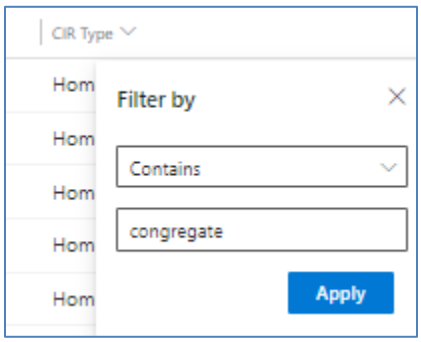


To view **filtering** options, click on *See all records* button at the top of the grid.



Click a column down arrow and click *Filter By*.

In the *Filter By* box, you have a variety of options. In this example, the user is filtering by Incident Report Types that contain the word 'congregate'.



Click *Apply* to view filtered results.

- Note regarding Dashboard view: you can change the size and visibility of the information on screen by using your browser zoom tools. Or, if using a mouse with a scroll wheel – click ctrl on your keyboard and move scroll wheel to zoom in/out.
- You can click the *Home* button at any time to return to the Dashboard view.

Inactivity Timeout

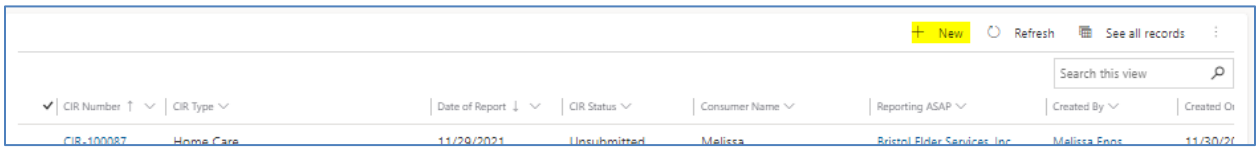
If a CIR System session is open and left idle for 20 minutes, the user will be automatically logged out. This is a data security measure. The user will lose any unsaved data entry and will need to log in again.

Submitting a Critical Incident Report

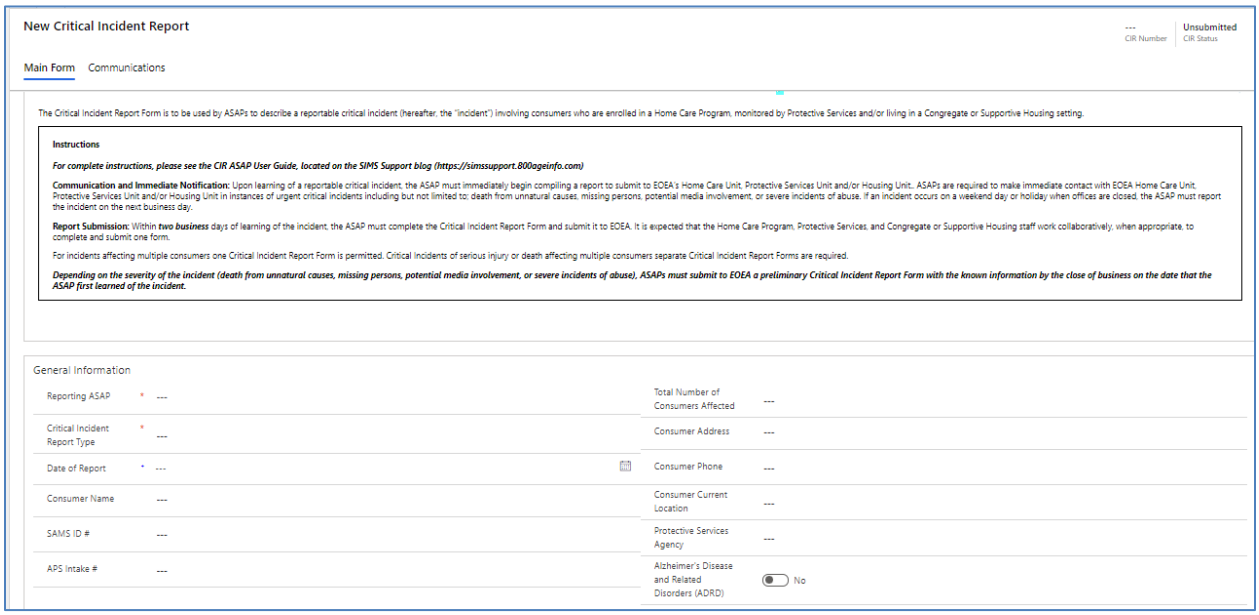
Follow established guidelines regarding what constitutes a critical incident and the required timeframe for reporting incidents. The new electronic CIR system is simply a change to the method of transmission and review of critical incident reports.

Steps to Submit New CIR

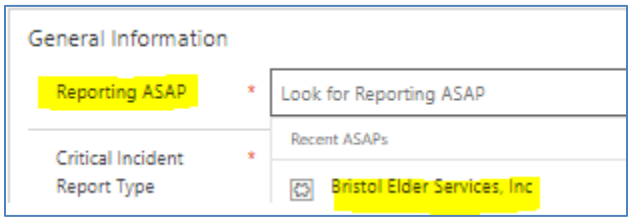
1. From the Dashboard home page, click *+ New* button, located above the Incident Report listing area.



2. A new, blank report will be displayed, ready to fill out. Note that standard instructions on critical incident reporting are posted at the top of the form.

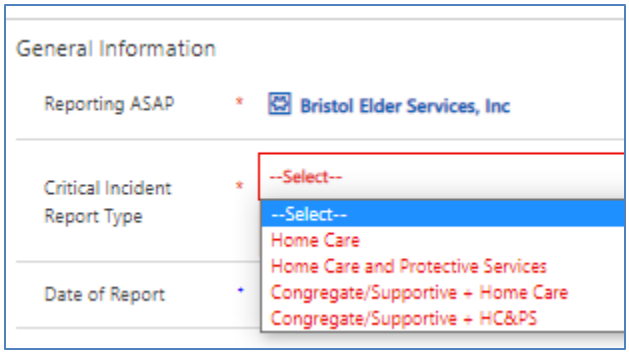


3. Fill in the Reporting ASAP field. Your agency should be the only one you can select in this field. This field is required before you can save the Incident Report. For agencies that are not ASAPs, you should still complete this field and your agency should be the only one you can elect in this field.



4. Select the type of Critical Incident Report you are submitting. What you see here will be determined by your user role. In this example, the user has the Home Care role, so they can only

see the Critical Incident Report types that include Home Care. This field also must be completed in order to save the Incident Report.

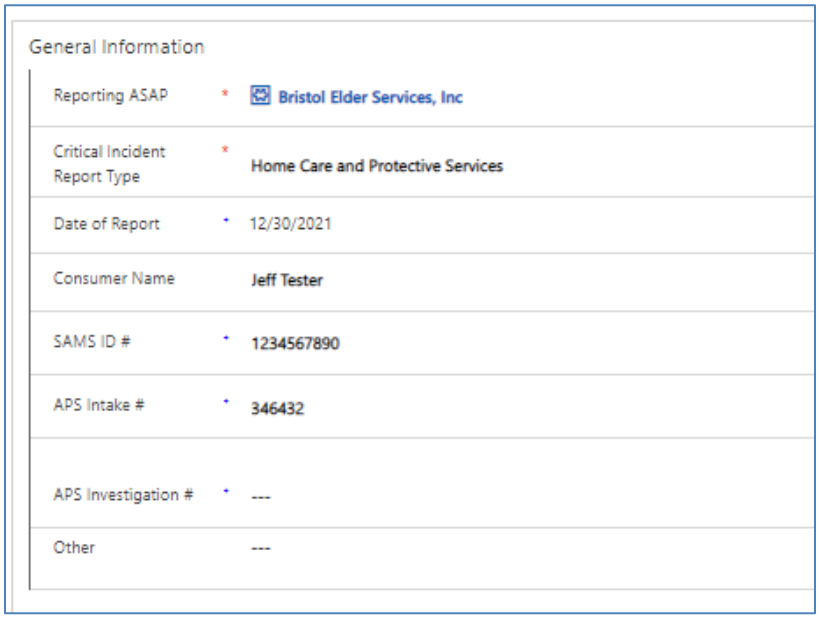


➲ To see a table with all the user roles and the types of Critical Incident Reports they can view, go to Appendix A.

5. Once you have entered ASAP (Agency) and Critical Incident Report type, you can save the Incident Report at any time and return to it later. Complete the **General Information** section as needed.

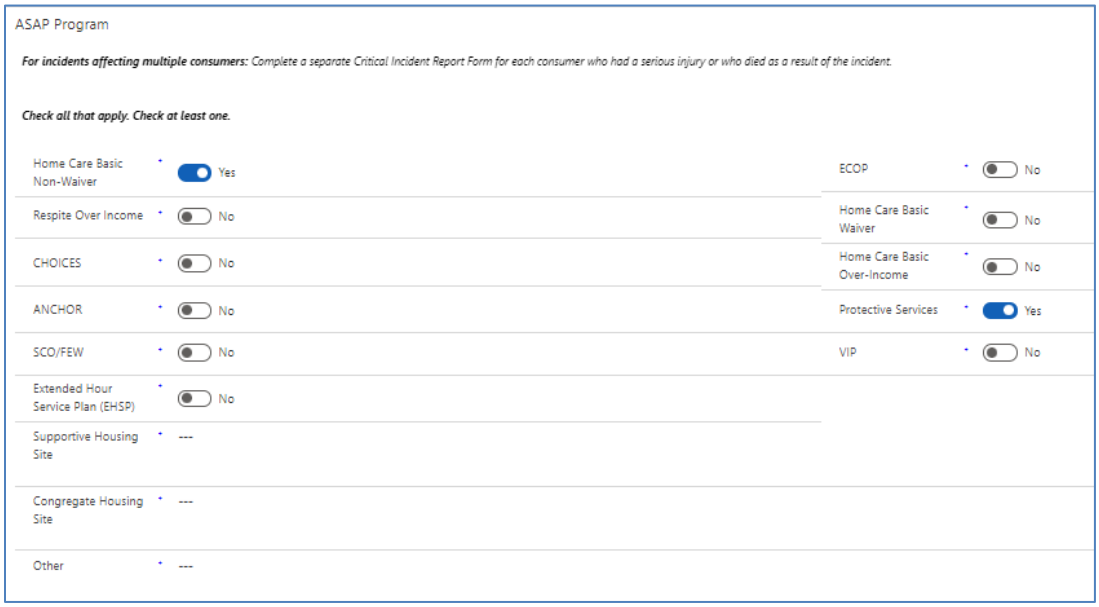
   Note that some fields are *required* in order to submit the Incident Report, and these fields vary depending on the type of Incident Report.

   For example, this user has selected the Home Care and Protective Services Critical Incident Report type and is therefore required to enter data in at least one of the following fields: SAMS ID #, APS Intake #, or APS Investigation Number.

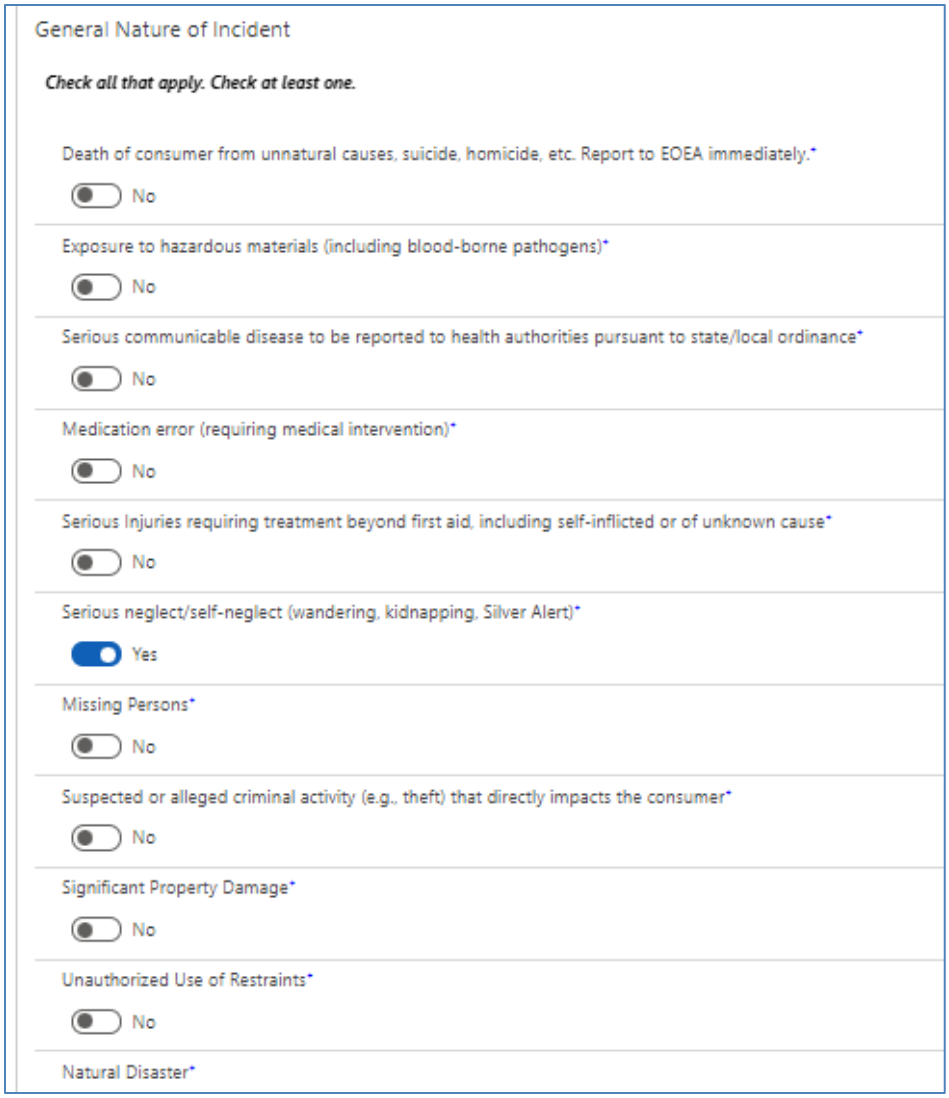


- If there are any required fields that that were left blank, the system will tell you specifically which ones when you attempt to submit.

6. In the ASAP (Agency) program section, you must select at least one program from the available options.



7. Same holds true for the **General Nature of Incident** section, at least one choice must be selected.


General Nature of Incident

Check all that apply. Check at least one.

Death of consumer from unnatural causes, suicide, homicide, etc. Report to EOEA immediately.*

No

Exposure to hazardous materials (including blood-borne pathogens)*

No

Serious communicable disease to be reported to health authorities pursuant to state/local ordinance*

No

Medication error (requiring medical intervention)*

No

Serious Injuries requiring treatment beyond first aid, including self-inflicted or of unknown cause*

No

Serious neglect/self-neglect (wandering, kidnapping, Silver Alert)*

Yes

Missing Persons*

No

Suspected or alleged criminal activity (e.g., theft) that directly impacts the consumer*

No

Significant Property Damage*

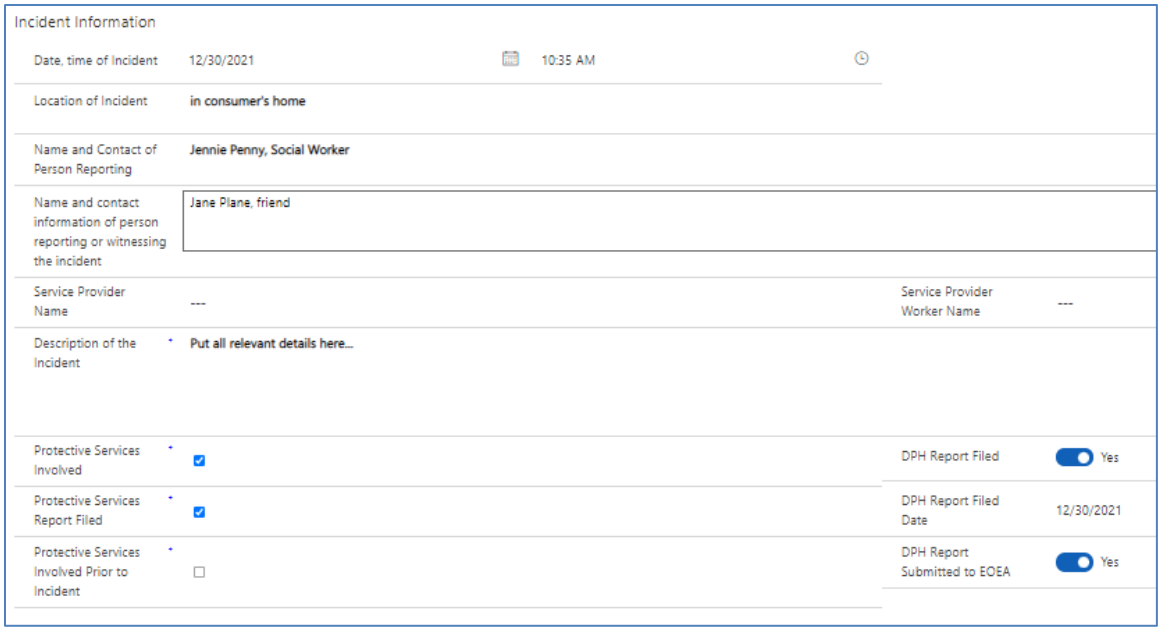
No

Unauthorized Use of Restraints*

No

Natural Disaster*

8. Fill in as much information as you have available in the Incident Information section, including a detailed description of the incident in the *Description of the Incident* text box.

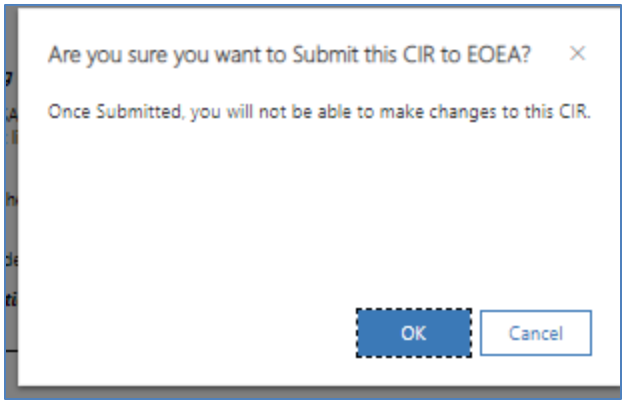


9. Complete the **Media**, and **Interventions and Outcomes** sections if relevant.

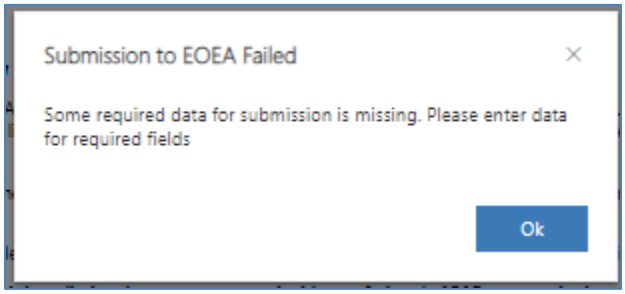
10. In the **Certification** section, note the required fields have a blue asterisk next to them, and that there is an additional field to list anyone else who was involved in completing the Incident Report.

➲ As noted, you can save the Incident Report and come back to it, as long as the ASAP (Agency) and Critical Incident Report Type fields are completed.

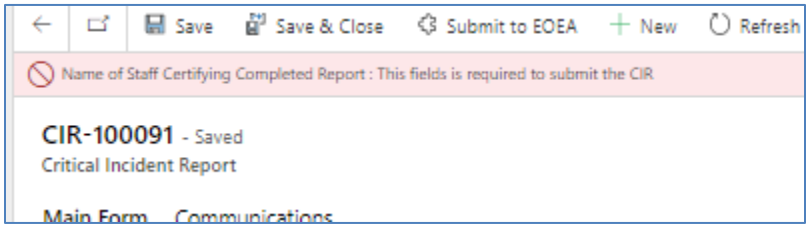
11. Once you believe the Incident Report is complete and ready to submit, click *Save*, and then *Submit to EOEA* at the top of the form. You will see this message:



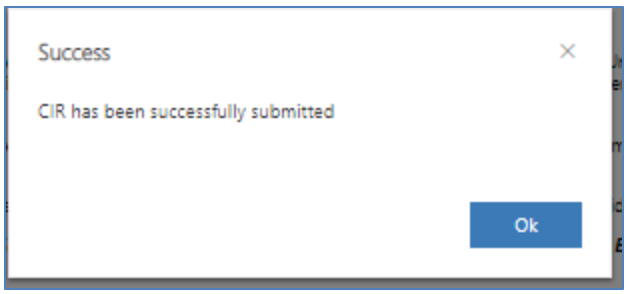
12. If a required field was not completed, you will see this message:



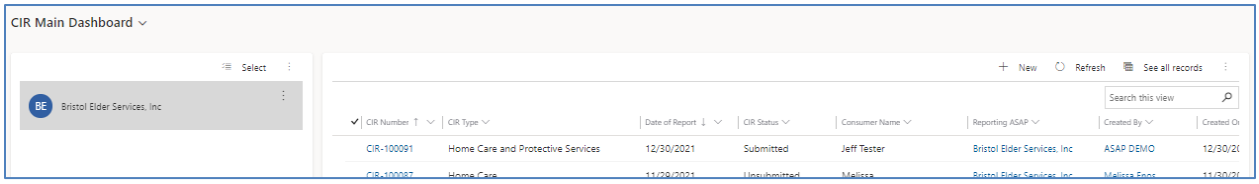
13. Click OK and you will see the reason(s) at the top of the screen. In this case the user forgot to enter the name of staff person completing Incident Report.



14. Add the required information and *Save*. Then click *Submit to EOEA* again. You should eventually see this message:



15. Returning to your dashboard, you should now see your recently submitted Incident Report at the top of the grid. Note that the status is now *Submitted*.



A Note About Incident Report Status Changes

Below are the possible statuses of an Incident Report in the CIR system:

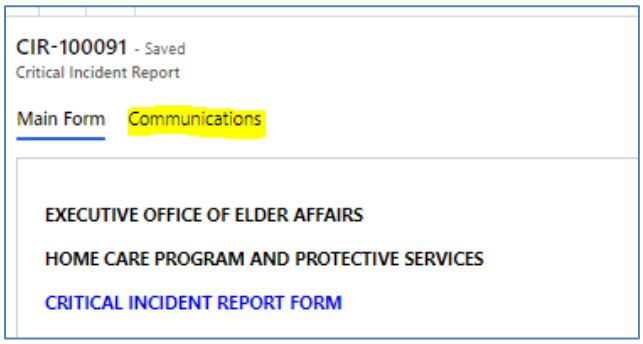
- Unsubmitted – Agency user can edit
- Submitted – Locked for editing
- In Progress – Locked for editing
- Completed – Locked for editing

If a situation arises where you have submitted an Incident Report but still need to add information after submitting, an EOEA user can change the status back to *Unsubmitted*. This will allow you to add the information and re-submit the Incident Report to EOEA.

Certain status changes will trigger an email notification to you. These scenarios are explained in the Email Notification section.

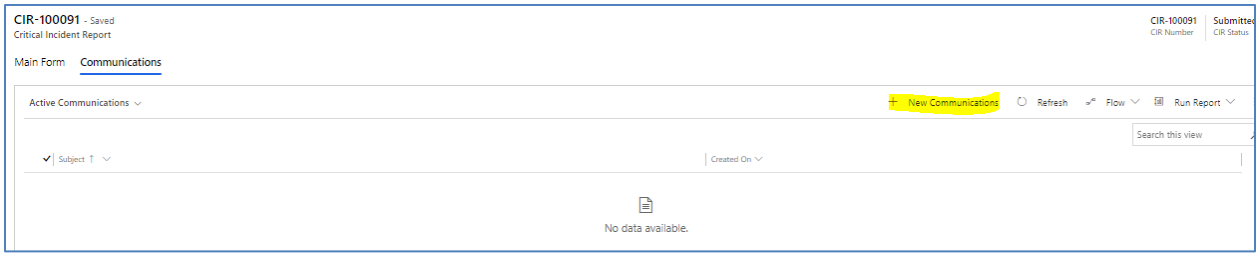
Communications and Attachments

The CIR System has a page dedicated to communication between the agency and EOEA for each submitted Incident Report. Communications in this context can be notes or attachments. The Communications page can be accessed from any open Incident Report, next to the Main Form tab.

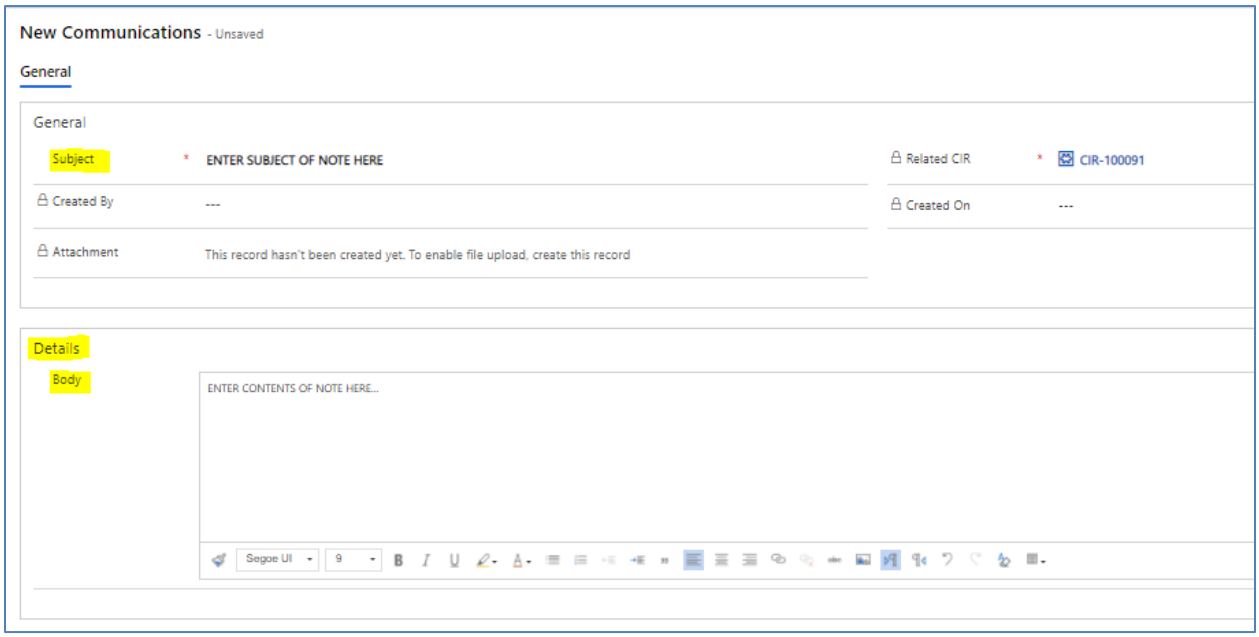


Adding a New Note

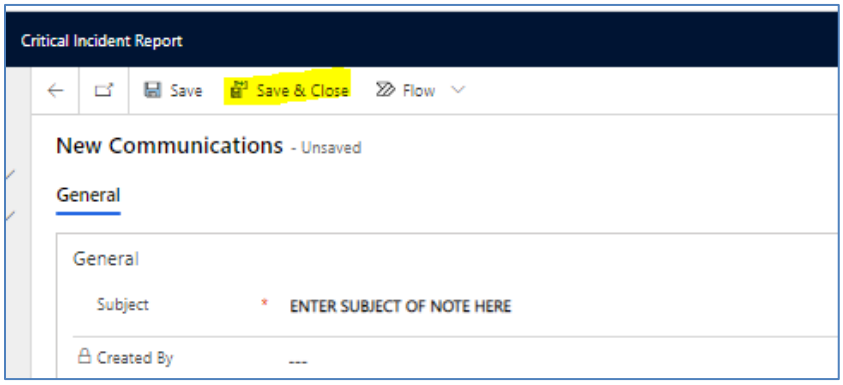
1. Click *Communications* tab within an open Incident Report
2. Click *+ New Communication* button



3. Enter brief description of note subject in the *Subject* field, then enter the contents of your note in the *Details/Body* text box below.



4. When complete, click *Save & Close*

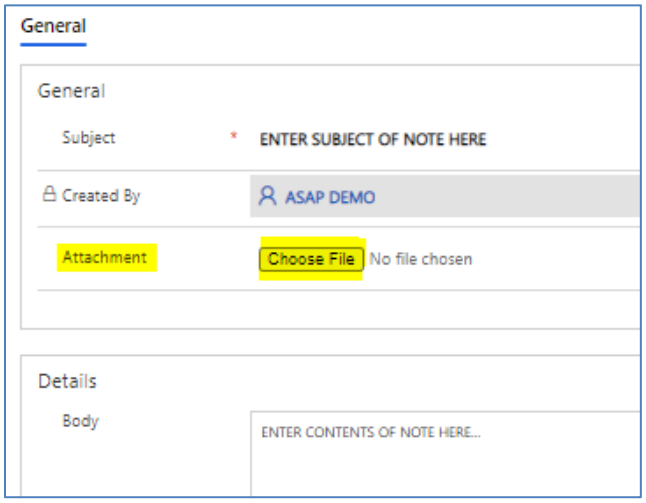


5. Use the browser back button to return to the Incident Report Main Form or click the *Home* button to go back to the *Dashboard*.

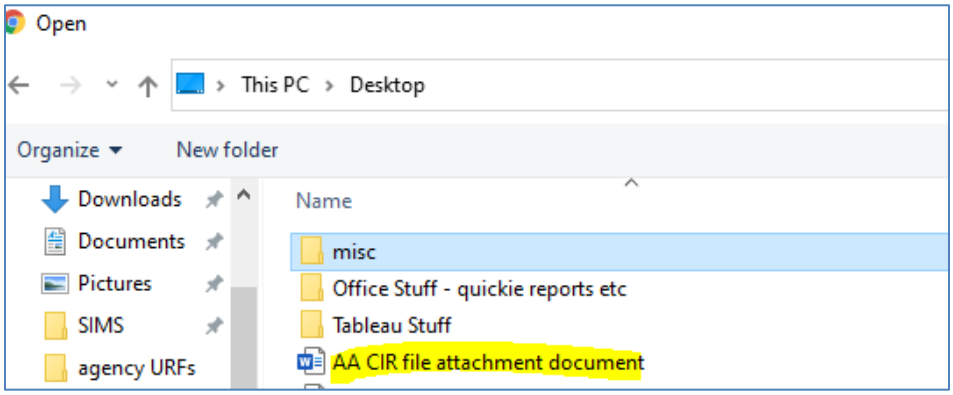
Adding an Attachment to a Note

To add an attachment, your note first must be *saved*.

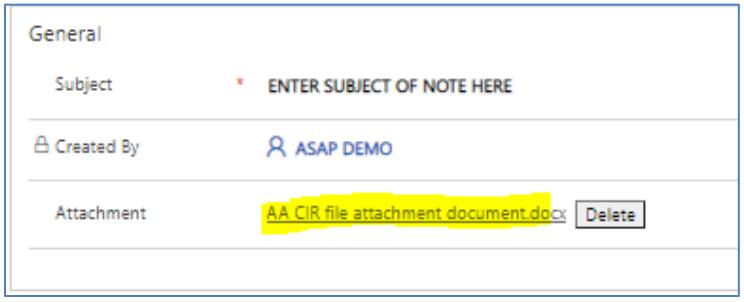
1. Click the *Choose File* button



2. Locate the desired document in your files, and double click it.



3. The document should now appear within the *Attachment* field of your note. *Save & Close*.



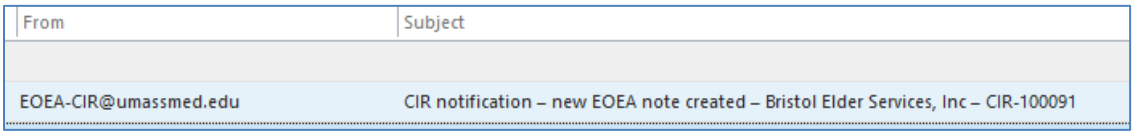
➲ Note: When adding an attachment, be sure to include text in the *Details* section describing the purpose of the attached document.

Email Notifications

The CIR System is set up to trigger emails to Agency and EOEA users under specific circumstances. These are the scenarios that would trigger an email to an Agency user:

1. When an EOEA user changes the status of an Incident Report that you submitted to CLOSED.
2. When an EOEA user changes the status of an Incident Report that you submitted to UNSUBMITTED. This allows you to edit the Incident Report and resubmit if necessary.
3. When an EOEA user adds a new note to an Incident Report that you submitted.

➲ Email notifications will appear in your email inbox as shown in the image below. The subject line includes the type of notification, your agency name, and the CIR ID number in the CIR System that the notification relates to.



CIR System Support

User Account Requests

All user requests – *new user, edit user, and revoke user*- should be submitted using the *CIR User Request Form.*

It is the responsibility of the agency to track and keep user list up to date, revoking user access for anyone who no longer requires it as soon as possible.

To submit a user request:

1. Download a CIR User Request Form (URF) from the *For Professionals* blog: https://forprofessionals.800ageinfo.com/critical-incident-reporting.html .
2. Enter date, request type (new/edit/revoke), agency, email address of user, and role desired.
3. Save the form for your records, and to use for your next request.

Submit form to EOEAHomeCareUnit@mass.gov for a **Home Care** related request, EOEAPSUnit@MassMail.mass.gov for **Protective Services**, or Emily.Cooper@mass.gov for **Housing Agencies***.

➲ Double check your form for accuracy including spelling, especially the email address.

➲ Know what IRs the role you are requesting allows a user to view. The IRs a user is allowed to view are determined by the user role. For example, if a user has the Home Care user role, they can only see IRs that *involve* Home Care. The same holds true, respectively, for Protective Services and Housing agency* users. See Appendix A for grid with details on roles and the IRs that can be viewed by each.

➲ *Housing is defined here as agencies that are contracted with EOEA to provide Congregate Housing services and are not ASAPs.

Contacting Support for Help with an Issue

For assistance with user access, a technical issue, or a question for EOEA program staff, contact the appropriate department email displayed below. Technical issues may be escalated to EOEA Support and the UMass software development team.

Home Care: EOEAHomeCareUnit@mass.gov

Protective Services: EOEAPSUnit@mass.gov

Housing: Emily.Cooper@mass.gov

Technical Recommendations

While the CIR System application will work with most browsers, we have found that Google Chrome functions well.

The new CIR system login is a Microsoft-hosted environment. Some users – but not all -- may also be using Microsoft-hosted environments to run other applications, which may include Microsoft Office 365 applications like email. If this is the case for you, we recommend that you attempt to access each of your Microsoft environments via a separate web browser (for example, make connections to your UMass application from a Chrome browser, and make connections to Microsoft email from an Edge browser). Another approach would be to completely log out from one Microsoft environment before launching a connection to the other.

Document History

Version	date	note	author
V1.0	1/3/22	First draft	Andy Grigorov
V1.0	1/13/22	Final draft approved	Andy Grigorov
V1.1	2/8/22	Edit to MS Auth. section	Andy Grigorov
V1.2	3/21/23	Updated first login and added self-serve pw instructions	Andy Grigorov

Appendix A

User Roles and the Incident Report types that Each Role Type Can View:

User Role	Incident Report Types role can view:
Home Care	Home Care HC & Protective Services HC & Housing HC & PS & Housing
Protective Services	Protective Services PS & HC PS & Housing PS & HC & Housing
Housing	Housing Housing & HC Housing & PS Housing & HC & PS

User Roles and the Incident Report types that Each Role Type Can View:

User Role	Incident Report Types role can view:
Home Care	Home Care HC & Protective Services HC & Housing HC & PS & Housing
Protective Services	Protective Services PS & HC PS & Housing PS & HC & Housing
Housing	Housing Housing & HC Housing & PS Housing & HC & PS

Appendix B

The following text is from the UMass Non-UMMS User Data Access Agreement, which all users must agree to upon first login.

Non-UMMS User Data Access Agreement

I acknowledge and agree that the security of the University of Massachusetts Medical School (UMMS) computer systems and the privacy and security of UMMS electronic data is of utmost priority. As a condition of obtaining access to UMMS systems and/or electronic data, I agree that I will:

1. Access and use UMMS systems and electronic data only as authorized; 2. Not transmit or post any information utilizing the UMMS system that is unrelated to or beyond the scope of my permission to utilize the system. 3. Keep confidential all information pertaining to the security of UMMS systems; 4. Treat as confidential all user IDs and passwords needed to gain access to UMMS systems or electronic data; 5. Not transmit personally-identifiable or confidential UMMS

data over open networks unless specifically authorized and unless encrypted; 6. Not attempt to access data which is not necessary to achieve the purpose of my access authorization; 7. Not attempt to discover the password(s) of any other UMMS user by any means; 8. Not circumvent or attempt to circumvent any security mechanism or procedure applicable to UMMS systems or to UMMS electronic data; 9. Not use UMMS systems to gain unauthorized access to any other computer system, or for any other unlawful purpose; 10. Not use UMMS systems to harass, threaten or stalk any individual; 11. Not install any applications on the UMMS system; 12. Not attempt to intercept or otherwise monitor any UMMS computer systems, including logins, email, or any other type of UMMS network traffic; 13. Not attempt to access UMMS-owned individually-identified, client, or personnel records, student grades or financial records, or any other UMMS electronic records reasonably expected to be confidential; 14. Accept responsibility for the preservation, privacy and security of UMMS data in my possession; 15. Immediately notify UMMS if I become aware of any actual or suspected security breach to UMMS systems and/or electronic data by calling: 508.856.8326. 16. Immediately notify UMMS if I receive UMMS data not intended for me and arrange for its secure return, re-transmission, or destruction, as UMMS directs; and 17. Comply with all applicable state and federal laws which govern the use and security of computer systems and data including but not limited to the Federal Copyright Law, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the Electronic Communications Privacy Act of 1986, the Computer Security Act of 1986, the Health Insurance Portability and Accountability Act of 1996, M.G.L. chapter 93H, and the Health Information Technology for Economic and Clinical Health Act of 2009.

I further acknowledge that the termination or expiration of my access to UMMS systems and/or electronic data will not relieve me of my obligations under this Agreement to keep confidential the personallyidentifiable data or UMMS network security information I may have accessed under this Agreement.

In case of conflict between this Agreement and any prior contracts between the parties, this Agreement will prevail.

_____

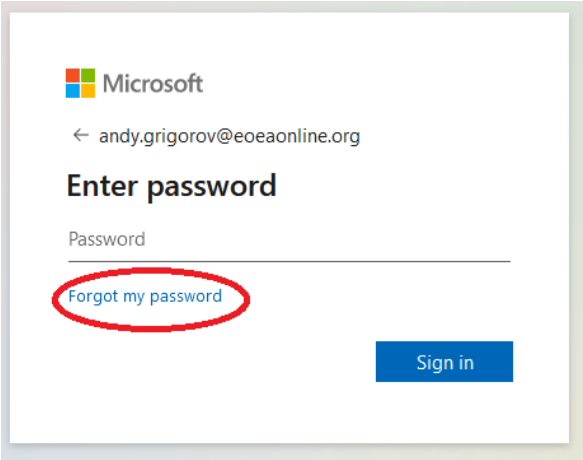
User (signature) Date

Acceptance of Agreement Online is equal to user's agreement to terms.

Appendix C – How to Reset Your Password

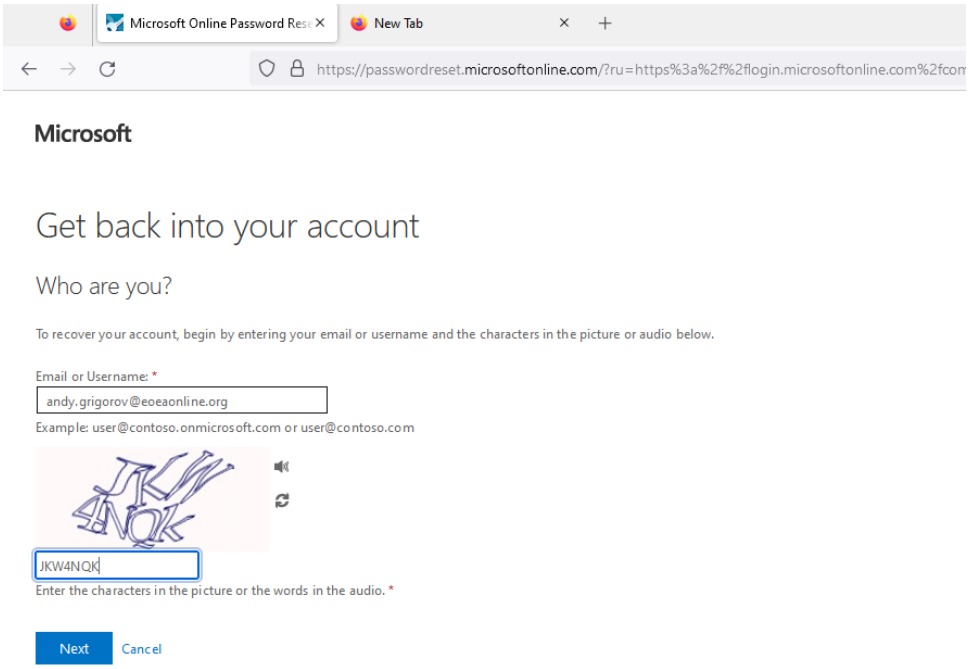
The new environment includes a convenient self-service password reset function. There are two ways to access this function:

- Click “Forgot my password” on the login page (https://myapps.microsoft.com), as shown below:

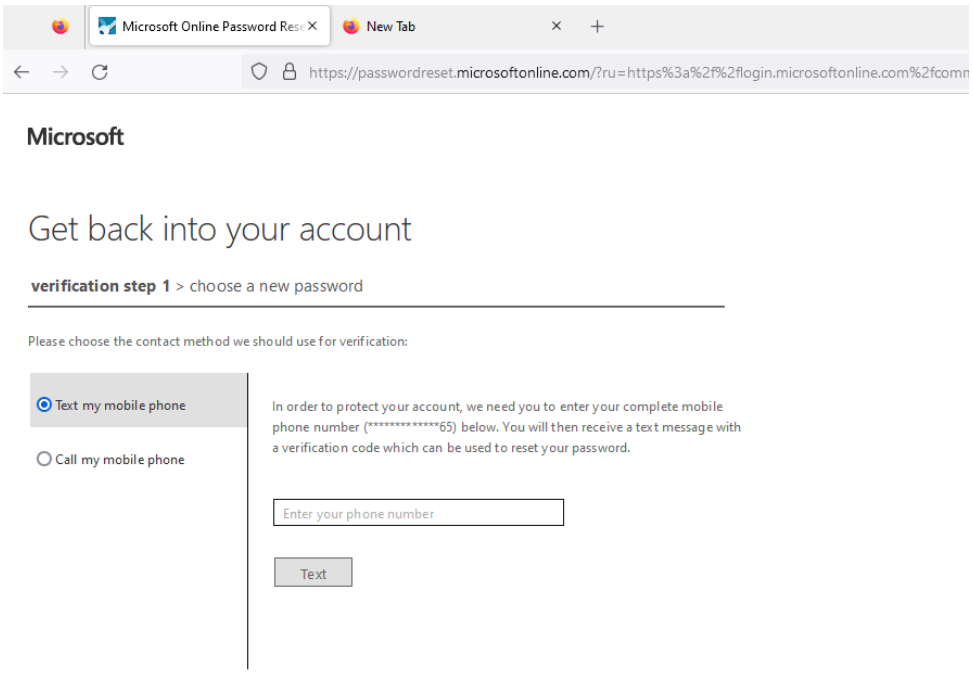


- Go directly to https://passwordreset.microsoftonline.com

Next, the "Get back into your account" prompt is displayed, as shown below. Provide responses to the prompts, and click Next.



Next, you'll be prompted to use one of the security access methods you specified during account setup, to verify your identify and reset your password (see image below).



After you've verified your identity, you'll be prompted specify your new password, as shown below: