Session Time Out ............................................................................................................... 36

Reports ................................................................................................................................ 37
  Detailed Report ................................................................................................................ 37
  LTCH Status Report ........................................................................................................ 39
  Home Geographical Status Report .............................................................................. 41
  CIS Data Report .............................................................................................................. 42

Security Awareness ........................................................................................................... 45
  Secure Practices for LTCHomes.net users ................................................................ 45
  Password Security ....................................................................................................... 45
  User Account Management .......................................................................................... 46
  Workstation Security .................................................................................................... 46
Critical Incident System
LTC Home user manual
Introduction

The Critical Incident System (CIS) is located on the [www.ltchomes.net](http://www.ltchomes.net) website, also known as the Long Term Care Homes Portal. This user guide will aid Long Term Care Homes, in navigating the various aspects of the CIS. The CIS was designed to help Long Term Care Homes securely submit their critical incident forms. The information gathered through the system is used to develop benchmarks and other tools for improvement and may assist in identifying opportunities to apply best practices. In 2008, it replaced the paper “unusual occurrence” forms in use, to create a more efficient reporting process and more consistent reporting practices. Since that time, in response to regulatory amendments, the system has undergone some changes to reflect new reporting requirements. This current version of the CIS, released in June 2016, includes minor form updates, improved functionality and a new look and feel.

CIS records may contain Personal Health Information which is protected by privacy legislation. Creating, viewing, or modifying a CI form or report on the CIS, requires a valid login ID and secure password. While ltchomes.net provides a secure environment for the reporting of Personal Health Information, all users also play a role in maintaining the security of these records. Please refer to the safe computing practices in the Security Awareness section of this manual for tips on how to keep critical incident records safe in an online environment.

There are three types of CIS users:

1. **LTC Home** user (LTC Home staff who submit and amend CI forms)
2. **SAO** user (Service Area Office staff of the Ministry of Health and Long-Term Care (MOHLTC) staff who review Critical Incidents as part of the Long-Term Care Inspection Program)
3. **System Admin** (MOHLTC staff that administer the system i.e. Health Data Branch)

Contacts:

For assistance, comments and general inquiries regarding the Critical Incident System please contact the Health Data Branch:

E-mail: commentsLTCH.MOH@ontario.ca

For assistance with user accounts on ltchomes.net (passwords, adding new users) please contact your LTC Home’s User Account Manager.
# Conventions Used in this Guide

The following table lists the typing conventions used throughout this document.

<table>
<thead>
<tr>
<th>Component</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Menu Items</strong></td>
<td>Menu items appear in bold and italic print. If several actions are to be performed in the menu, they are linked with a horizontal arrow→. Example: <em>File→Save</em></td>
</tr>
<tr>
<td><strong>Field Names</strong></td>
<td>Field names appear in caps. Example: USER ID</td>
</tr>
<tr>
<td><strong>Screen Names</strong></td>
<td>Screen names are italicized. Example: <em>Select Submission File</em></td>
</tr>
<tr>
<td><strong>Buttons and icons</strong></td>
<td>Buttons and icons appear as they do on the screen</td>
</tr>
<tr>
<td><strong>Click</strong></td>
<td>Click refers to clicking the left mouse button when you have selected a menu option, item or icon.</td>
</tr>
<tr>
<td><strong>Select</strong></td>
<td>Select refers to selecting a menu option or an item</td>
</tr>
</tbody>
</table>
# Definitions

## Search CI screens

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI Form Number</td>
<td>The unique number automatically assigned to each CI form.</td>
</tr>
<tr>
<td>Date of CI</td>
<td>The Date the Critical Incident occurred.</td>
</tr>
<tr>
<td>Status</td>
<td>The current submission status of the form. The status may be one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Saved:</strong> These forms have not yet been submitted to the MOHLTC and can only be viewed by LTC Home users. Forms with this status can be edited. The system deletes the form 12 days after creating it, if it has not been submitted. The Home users who receive CIS email notifications will receive a reminder email asking for submission. These emails include ‘CI Deletion Initiated’ in the subject line.</td>
</tr>
<tr>
<td></td>
<td><strong>Submitted:</strong> Forms with this status have been submitted to the MOHLTC for the first time.</td>
</tr>
<tr>
<td></td>
<td><strong>Amended:</strong> Forms with this status are already submitted but a home has added additional information.</td>
</tr>
<tr>
<td></td>
<td><strong>Finalized:</strong> This status only applies to Disease Outbreak CI forms. When a LTC Home enters a ‘Date Declared Over’ for the reported Disease Outbreak, the status of the CI becomes Finalized and the form can no longer be amended.</td>
</tr>
<tr>
<td>CI Type</td>
<td>The type of CI or Mandatory Report that the form documents.</td>
</tr>
<tr>
<td>Home</td>
<td>Name of the LTC Home.</td>
</tr>
<tr>
<td>Area</td>
<td>LHIN or SAO where the home is located.</td>
</tr>
</tbody>
</table>
## Report CI screens

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>LHIN or SAO where the home is located.</td>
</tr>
<tr>
<td>Home</td>
<td>Name of the LTC Home.</td>
</tr>
<tr>
<td>From</td>
<td>The Date the Critical Incident occurred.</td>
</tr>
<tr>
<td>To</td>
<td>The Date the Critical Incident occurred.</td>
</tr>
<tr>
<td>Status</td>
<td>The current submission status of the form.</td>
</tr>
<tr>
<td>Sector</td>
<td>Municipal, Nursing Home for the Aged</td>
</tr>
<tr>
<td>Type</td>
<td>Sub-Type</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Mandatory Reports</strong></td>
<td></td>
</tr>
<tr>
<td>Abuse/Neglect [24(1)(2)]</td>
<td>Resident to Resident</td>
</tr>
<tr>
<td></td>
<td>Visitor to Resident</td>
</tr>
<tr>
<td></td>
<td>Staff to Resident</td>
</tr>
<tr>
<td>Improper/Incompetent treatment of a resident that results in harm or</td>
<td></td>
</tr>
<tr>
<td>risk to a resident [24(1)(1)]</td>
<td></td>
</tr>
<tr>
<td>Misuse/Misappropriation of residents money [24(1)(4)]</td>
<td></td>
</tr>
<tr>
<td>Unlawful conduct that resulted in harm/risk of harm to resident</td>
<td></td>
</tr>
<tr>
<td>[24(1)(3)]</td>
<td></td>
</tr>
<tr>
<td>Misuse/Misappropriation of funding provided to a licensee [24(1)(5)]</td>
<td></td>
</tr>
<tr>
<td><strong>Critical Incidents</strong></td>
<td></td>
</tr>
<tr>
<td>Unexpected Death [107(1)(2)]</td>
<td></td>
</tr>
<tr>
<td>Disease Outbreak [107(1)(5)]</td>
<td>Acute Respiratory Illness (ARI)</td>
</tr>
<tr>
<td></td>
<td>Enteric Illness</td>
</tr>
<tr>
<td></td>
<td>Antibiotic Resistant Organism (ARO) – MRSA</td>
</tr>
<tr>
<td></td>
<td>Antibiotic Resistant Organism (ARO) – VRE</td>
</tr>
<tr>
<td></td>
<td>Antibiotic Resistant Organism (ARO) – ESBL</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Incident that causes an injury to a resident for which the resident</td>
<td>Fracture</td>
</tr>
<tr>
<td>is taken to hospital and which results in a significant change in the</td>
<td></td>
</tr>
<tr>
<td>resident’s health status [107(3)(4)]</td>
<td>Fall</td>
</tr>
<tr>
<td></td>
<td>Bruising</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Medication incident/adverse drug reaction [107(3)(5)]</td>
<td>Errors in administering that alter a resident’s health status</td>
</tr>
<tr>
<td></td>
<td>Adverse reaction that alter a resident’s health status</td>
</tr>
<tr>
<td></td>
<td>Misappropriation</td>
</tr>
<tr>
<td>Emergency [107(1)(1)]</td>
<td>Bomb threat</td>
</tr>
<tr>
<td></td>
<td>Fire</td>
</tr>
<tr>
<td></td>
<td>Unplanned Evacuation (partial or full)</td>
</tr>
<tr>
<td></td>
<td>Intake of evacuees</td>
</tr>
<tr>
<td></td>
<td>Strike (Staff Shortage)</td>
</tr>
<tr>
<td></td>
<td>Pandemic</td>
</tr>
<tr>
<td></td>
<td>External Chemical Spill</td>
</tr>
<tr>
<td></td>
<td>External Air Quality</td>
</tr>
<tr>
<td></td>
<td>Severe Weather</td>
</tr>
<tr>
<td></td>
<td>Violent Outburst</td>
</tr>
<tr>
<td>Environmental Hazard [107(3)(2)]</td>
<td>Failure/breakdown of major equipment</td>
</tr>
<tr>
<td></td>
<td>Failure/breakdown of major system</td>
</tr>
<tr>
<td></td>
<td>Loss of essential services</td>
</tr>
<tr>
<td></td>
<td>Flooding</td>
</tr>
<tr>
<td></td>
<td>Other</td>
</tr>
<tr>
<td>Missing Resident &gt;= 3 Hours [107(1)(3)]</td>
<td></td>
</tr>
<tr>
<td>Missing Resident &lt;= 3 Hours [107(3)(1)]</td>
<td></td>
</tr>
<tr>
<td>Missing Resident with Injury [107(1)(4)]</td>
<td></td>
</tr>
<tr>
<td>Controlled Substance missing/unaccounted [107(3)(3)]</td>
<td></td>
</tr>
<tr>
<td>Contamination of drinking water supply [107(1)(6)]</td>
<td></td>
</tr>
</tbody>
</table>
Accessing the CIS

Signing In

Go to the Long Term Care Homes Portal by copying the following link https://www.ltchomes.net/LTCHPortal/Login.aspx in the address bar of your internet browser and pressing ENTER on your keyboard. [Screen 1]

The Login screen of ltchomes.net will be displayed [Screen 2]. Enter your Login ID and your Password, and click the ‘Signin’ button.
If you are a **new** CIS user, you will be presented the Terms of Use [Screen 3]

1. Review and accept in order to proceed.

![Screen 3](image)

The password provided to you is temporary and upon accepting the Terms of Use, the Change Password screen will appear. [Screen 4]

![Screen 4](image)
2. Enter the password provided to you in the Old Password field.

3. Enter a password of your choice in the New Password field and Confirm New Password Fields. Password guidelines are listed on the right hand side of the screen [Screen 5].

   **Password Guidelines**
   - Be at least 8 characters long
   - Contain at least 3 of the 4 following types of characters:
     1. UPPER CASE LETTERS
     2. lower case letters
     3. digit(s) from 0 to 9
     4. special characters (e.g., @ # $ % ^ & =)
   - Not use the same first four characters as your User ID
   - Not be the same as your old password

   Screen 5

4. Click ‘Update’.

5. You will receive a message

   ![You have successfully changed your password.]

6. Click the ‘Proceed’ button.

The Security questions screen will appear. [Screen 6]
7. Select 5 security questions and complete the answers.

8. Click the ‘Save’ button.

If you are an existing user and you have forgotten your password, click the ‘Forgot Your Password?’ link for help accessing the system. Using your security questions, you will have the opportunity to create a new temporary password. This password must be changed at the next login. Your user account manager can also reset your password. When your password is reset, you must recreate your five security questions/answers.

Once logged in, the Select Organization screen will open [Screen 7]. Click the name of the organization to highlight it and then click the ‘Select’ button.

The LTCHomes.net Home page opens. Under Applications, select CIS – Critical Incident System [Screen 8].
You will be asked a randomly selected security question [Screen 9]. Please note you will only be asked one security question per session on LTCHomes.net.

The Critical incident System Menu opens.
Navigation

There are four menu items in the Critical Incident System [Screen 10]:

1. **Create New** – Submitting a new Critical Incident/Mandatory Report
2. **Search** – Searching existing Saved/Submitted/Amended Forms
3. **Training Manual** – Downloading the CIS User Guide
4. **Reports** – Summary Reports
Reporting a New Critical Incident

Under the *Create New* menu, you can submit a new Critical Incident Form to the MOHLTC.

1. From the Critical Incident System main menu, under *Create New*, select *Report New Critical Incident*.

2. The *Critical Incident Form* screen loads [Screen 11].

   1. Select your LTC Home from a drop down menu.

   2. In the DATE OF CI field, enter the date the Critical Incident occurred in the format (MM/DD/YYYY).

   3. In the TIME OF CI field, enter the time the Critical Incident occurred in the format (HH:MM).
4. Identify if you are reporting a Mandatory Report or a Critical Incident. If you are not sure, please look at the list to the right. If you select ‘Critical Incident’, the corresponding report types will be displayed.

5. Select which Mandatory Report or Critical Incident that best applies.

Note: All of these five fields are required. You must complete all fields to advance to the next step.

6. Click ‘Next’

A new screen opens with the Critical Incident Form Number. The ‘Date of CI’ and ‘Time of CI’ entered are also shown. [Screen 12]

Form questions appear below and are specific to the Mandatory Report or Critical Incident selected.

7. Answer each question and click ‘Save and Proceed’ to move to the next section.

8. Mandatory questions are indicated with red coloured text ‘(Required)’

9. If you click ‘Save and Proceed’ without completing a mandatory field or if the data you entered does not match the correct format, the field will be highlighted in red [Screen 13]

10. Text boxes have a 7000 Character Maximum. Any characters over 7000 will be erased from the system. If more information is required to be supplied, contact the Centralized Intake
Assessment and Triage Team (CIATT) for further instruction.

11. If entering information in the **Identifying Information** section, click the ‘Add’ button after entering each individual’s details. If you forget to click ‘Add’, the information will not be saved. [Screen 14]

12. If the MOHLTC after hours pager was contacted prior to reporting the incident in the CIS, enter the report number that was provided on the call. [Screen 15]
13. For resident-related occurrences, if relative(s), friends, designated contact(s) and/or substitute decision maker(s) were contacted, click the ‘Add’ button after entering each individual’s details. [Screen 16]

14. After the final question on the form, click ‘Save and Proceed’. A ‘Submit’ button will appear.

15. Click the ‘Submit’ button

You will receive a message confirming the report was submitted [Screen 17]

16. Click ‘OK’

17. You will be returned to the CI Search screen with all of your LTC Home’s reports listed. The most recently modified report will appear at the top.

18. A CI email notification is sent automatically from the system. See section ‘Critical Incident Email Notifications’ for more information on the email notifications and users who receive them.
**CI Form Attachments**

Additional documents can be added to the CI form as attachments and transmitted securely through the system to the MOHLTC.

1. To add an attachment, select the ‘Attachments’ icon at the top right hand corner of the CI form [Screen 18].

   ![Screen 18](Critical Incident Form Screen 18)

2. The attachment window appears [Screen 19]

   ![Screen 19](CI Form Attachment Screen 19)

3. Enter a Name for the file in the FILE NAME field.
4. Browse to the location of the file on your computer. Select the file and click the ‘Open’ button. [Screen 20]
5. In the attachment window, click the ‘Upload’ button. Your attachment will appear to the right hand side. [Screen 21]

6. Click ‘Close Window’
Searching for Critical Incident Forms

Under the Search menu, you can view a list of CI forms and the status of each.

1. In the Search menu, select Search for Critical Incidents.

2. The CI Search screen loads [Screen 22].

3. In the HOME field, enter the first few letters of the Home Name and the name will appear. Select the Home Name. When searching, complete as many of these fields as you wish. The more fields that are filled in, the more targeted the search will be. To generate a list of all CI forms that you have permissions to, you may leave all fields blank and click the ‘Search’ button.

4. Note that DATE OF CI, is the date the critical incident was reported as occurring.

5. Click the ‘Search’ button. Search results load in the area below the search criteria. [Screen 23]
Click the ‘View’ link to open the
Click the ‘Notes’ link to open the

To view the details of any form, click the *View* link. The report will open in a new window.

To view the Notes of any form, click the *Notes* link. The Notes window will open.
Viewing Critical Incident Forms

As mentioned on page 21, critical incident reports can be retrieved and viewed using the *Search for Critical Incidents* option. This requires the user to login to LTCHomes.net and access the CIS. CI reports can also be viewed by clicking on the report link in the CI email notification. CI notifications are automatically sent from the system when a report is submitted or amended. If you currently have an active CIS session open, clicking on the link will open the report directly in a new window. [Screen 24]

Note: If you are not yet logged in to LTCHomes.net, clicking on the link will open the ltchomes.net Sign in page. You will be required to answer a security question before accessing the CIS and viewing the form.

Amendments since the last submission are highlighted in red.

Any notes corresponding to a CI form will be located at the bottom of the form [Screen 25].
Attachments are also located at the bottom of the form. To access the attachments click on the Filename [Screen 26].

To return to the main CIS menu click the ‘Home’ menu at the top of the page.
Amending Critical Incident Forms

If you need to amend a previously submitted report, see the section of this guide entitled ‘Searching for Critical Incidents’ for steps on how to retrieve the report.

1. In the search results, click the ‘Edit’ link. [Screen 27]

   ![Screen 27]

2. The report will open in a new window.

   To make a change you must click the ‘Edit’ button [Screen 27] for the section you are updating. Please note, some sections cannot be modified after the report has been submitted, to maintain the integrity of the report type.

3. When editing a section of the report, the button will change to read ‘Currently editing’ [Screen 27]. Please note, you can only edit one section of the form at a time.

4. For text fields, click the ‘Add More’ button [Screen 27] to add information. Text entered in previously submitted reports cannot be deleted. Please enter additional information as required.

5. Make any changes needed and click the ‘Save and Proceed’ button [Screen 27].

6. To cancel the edit session, click the ‘Cancel’ button [Screen 27].
7. When amending a Critical Incident, as soon as you click ‘Save and Proceed’ in your edit session, a CI email notification will be sent automatically from the system indicating that an amendment was made. You may then proceed to make additional changes within the same session. Only one email will be sent for each amending session.

Locked Forms

CI forms are locked one year after the submission date. This is done to preserve the integrity of historical data and avoid amendments being made to incorrect forms. Locked forms are indicated with a lock icon. These reports can be opened and viewed by both SAO users and LTC Home users but cannot be amended by LTC Homes. SAO users can add notes to locked reports in the event information must be added to the report one year after the date it was submitted.

Note: As of June 1, 2016, when this version of CIS was released, all previously submitted CIs were locked from further amendments to accommodate the release of the new format. LTC Homes can add notes to these historical reports in the event additional information is required to be added.
Reporting Disease Outbreaks

Disease Outbreaks are unique forms in that their status can be ‘Finalized’. The action of entering a ‘Date Declared Over’ on the CI form changes the status to ‘Finalized’ and triggers an email notification. It also locks the form to prevent any further changes.

If the Outbreak has been declared by Public Health,
1. Follow the steps in section ‘Reporting a New Critical Incident’ to submit the form to the MOHLTC.
2. A CI email notification will be sent from the system, indicating the form status of Submitted.

If updates to the MOHLTC are required during the outbreak,
1. Follow the steps in section ‘Amending Critical Incident Forms’ to edit your CI form.
2. A CI email notification will be sent from the system, indicating the form status of Amended.

If the Outbreak has been declared over by Public Health,
1. Follow the steps in section ‘Amending Critical Incident Forms’ to edit your CI form.
2. Click the ‘Edit’ button to enable an edit session on any particular section of the form.
3. Make any final updates to the form.
4. Navigate to the bottom of the form. Ensure you click the ‘Edit’ button of the last form section. Enter the ‘Date Declared Over’.
5. You will receive a warning message [Screen 28]
6. Click the ‘OK’ button to finalize the form or the ‘CANCEL’ button to return to the form to make further updates.

7. If you clicked ‘OK’, a CI email notification will be sent from the system, indicating the form status of ‘Finalized’.

Please note that if there are multiple Disease Outbreaks occurring at your LTC Home, a separate form must be submitted for each one.
Notes

LTC Homes can’t add notes to CIs with the exception of Disease Outbreak forms after they are finalized. If information must be added to other CI form types, an amendment to the form body must be made.

The Notes window allows users to enter and view notes. The Notes window can be accessed in two ways:

1) After searching for a CI report, click on the Notes link on the far right hand side on the search results [Screen 29].

Screen 29

2) When viewing an open CI report, click on the ‘Notes’ button that appears at the top right of the report [Screen 30].

Screen 30

The Notes window appears [Screen 31].
1. Enter a note in the text box

2. Click the ‘Submit’ button

   The message appears:

   ![Image showing 'Your record saved successfully.']

   The note appears in the Note Thread on the right hand side. [Screen 32]

3. Click Close Window.

4. A CI email notification will be automatically sent from the system.

The subject line of the email is in the following format:

**NOTE ADDED** – CI ‘Status’ – ‘LONG TERM CARE HOME NAME’ – ‘CI Type’ (‘Form No’)

Email notifications are sent to the Centralized Intake Assessment and Triage Team, and LTCHomes.net users with the following roles:
• Home Administrator
• Director of Care

For Disease Outbreak forms, email notifications will also be sent to the following role:
• Environmental Advisor
Request for Amendments

Once a submitted CI form is reviewed by the Centralized Intake Assessment and Triage Team, a request for additional information may be required.

Notes are added to CI forms by SAO users for this purpose. When a request for amendment is made, the Inspection Team will add a Note and send an email notification to LTChomes.net users at the Long-Term Care Home.

The subject line of the email is in the following format:

REQUEST FOR AMENDMENT - CI ‘Status’ - ‘LONG TERM CARE HOME NAME’ - ‘CI Type’ (‘Form No’)

To View the Note,

1. Login to LTCHomes.net and access the Critical Incident System
2. Search for the report
3. Click on the Notes link on the far right hand side on the search results [Screen 33].

4. The Notes window will open.

5. Alternatively, click on the View link. The report will open in a new window.

6. Scroll to the bottom of the form to view the Notes.

8. To add information to the report, in response to the Note, follow the steps in section ‘Amending Critical Incident Forms’ to edit your CI form.
Critical Incident Email notifications

Email notifications are automatically sent from the CIS when:

- submitting/amending a CI form
- finalizing a Disease Outbreak form when the outbreak has been declared over by Public Health
- a Saved report will be deleted if not Submitted
- SAO staff requests an Amendment (see page 28)
- a Note is added to a finalized Disease Outbreak form (see page 32-33)

When submitting/amending a CI or finalizing a Disease Outbreak, the subject line of the CI email notification contains information on the form status, form number, LTC Home and date.

CI 'Status' – ‘LONG TERM CARE HOME NAME’– ‘CI Type’ (‘Form No’) date [Screen 34]

Screen 34

Email notifications are sent to users of the LTC Homes Portal based on the CI type and user permissions. When submitting and amending all CI forms, and finalizing Disease Outbreaks, email
notifications are sent to the Centralized Intake Assessment and Triage Team, and LTCHomes.net users with the following roles:

- Home Administrator
- Director of Care

When submitting Abuse/Neglect, Emergency and Unexpected Death CI types, users with the following roles also receive the notification:

- SAO Manager
- LTCH Director under the Act

When submitting Environmental Hazard, Emergency, Disease Outbreak, Contamination of Drinking water supply and Controlled Substance missing/unaccounted CI types, users with the following role also receive the notification:

- Environmental Advisor

**CI Deletion**

Saved reports will be deleted automatically from the system, if not submitted within 12 days. The system will send a warning message in the days leading up to the deletion of the saved version. The subject line of the CI email notification contains ‘CI Deletion Initiated’, information on the form number, LTC Home and date.

Example:
CI Deletion Initiated - FIELDSTONE COMMONS CARE COMMUNITY - Abuse/Neglect [24(1)(2)] (2906-000005-16)

If you do not want to lose the saved version, please Submit the report before the deadline as stated in the body of the email. [Screen 35]
A security feature of the CIS is an automated session time out. This prevents unauthorized users from gaining access to the system if the user has left their workstation with the CIS running. If the system is left idle for 20 minutes, you will be automatically logged out of the CIS. On the top left hand corner of the CIS window the time left idle before session expiry is shown.

When your session is about to expire, a warning message will appear. You will be given the option to restart your session. Please note, when you are typing in a text box, the system does not recognize this as activity and you may be issued a warning.

Click ‘Ok’. Once you accept the warning, you will be able to continue working without loss of any information.
Reports

There are pre-defined reports available to Long-Term Care Homes that can be used to summarize CI data.

Detailed Report

The Detailed Report is used to generate a document containing one or more CI forms.

1. Select the Reports menu on the main CIS menu.
2. Select Detailed Report. The Detailed Report opens in a new window. [Screen 38]

3. The search options determine how many CI forms will be part of the report. The FROM and TO date fields must be filled in but all other fields are optional. The more fields that are filled in the more targeted the search will be. For example, if 01/01/2012 is entered as the From date and 10/17/2012 is entered as the To date and nothing is specified for the Home or Area fields, the report that will be generated will contain the details of all critical incidents from Jan. 1, 2012 to Oct. 17, 2012, for every home the user has permission to view data from.

4. Click the ‘View Report’ button. The report appears below the search fields. [Screen 39]
5. To save or print a copy of the report, click the Export button and select the appropriate file format. [Screen 40]
6. Click Open, Save or Save As, and browse to the appropriate folder on your computer. Open the report and print from the application selected.

7. To return to the main CIS menu click ‘Home’ at the top of the page.

**LTCH Status Report**

The *LTCH Status Report* generates a summary list of critical incidents by type and by status.

1. Select the *Reports* menu on the main CIS menu.
2. To view the LTCH Status Report click on *LTCH Status Report*. The screen to generate a report opens in a new window. [Screen 41]

   ![Screen 41](image)

3. The search options determine what data will be part of the report. The more fields that are filled in, the more targeted the report will be. The FROM and TO date fields are required, all other fields are optional. The report loads in the white space below the search options.

4. Click the ‘View Report’ button. The report appears below the search fields. [Screen 42]
5. To save or print a copy of the report, click the Export button and select the appropriate file format. [Screen 43]
6. Click Open, Save or Save As, and browse to the appropriate space on your computer. Open the report and print from the application selected.

7. To return to the main CIS menu click ‘Home’ at the top of the page.

**Home Geographical Status Report**

The *Home Geographical Status Report* generates a summary list of critical incidents by type and by area.

1. Select the *Reports* menu on the main CIS menu.
2. Select the *Home Geographical Status Report*. The screen to generate a report opens in a new window. [Screen 44]

3. The search options determine what data will be part of the report. The HOME, YEAR and QUARTER fields are required.

4. Click the ‘View Report’ button. The report appears below the search fields. [Screen 45]
5. To save or print a copy of the report, click the Export button and select the appropriate file format. [Screen 46]

![Screen 46]

6. Click Open, Save or Save As, and browse to the appropriate space on your computer. Open the report and print from the application selected.

7. To return to the main CIS menu click ‘Home’ at the top of the page.

**CIS Data Report**

The *CIS Data Report* is used to generate a summary report of CI forms by Area and Type. This document can be printed or saved to a secure location on your computer.

1. Select the **Reports** menu on the main CIS menu.
2. Select the **CIS Data Report**. The CIS Data Report screen opens in a new window. [Screen 47]
3. The search options determine how many CI forms will be part of the report. The START DATE and END DATE fields must be filled in, but all other fields are optional.

4. Click the ‘View Report’ button. The report appears below the search fields. [Screen 48]

5. To save or print a copy of the report, click the Export button and select the appropriate file format. [Screen 49]
6. Click Open, Save or Save As, and browse to the appropriate space on your computer. Open the report and print from the application selected.

7. To return to the main CIS menu click ‘Home’ at the top of the page.
Security Awareness

The LTChomes.net web portal (Portal) houses Personal Information (PI) and/or Personal Health Information (PHI) in the Critical Incident System (CIS). PI (e.g. resident name & address) and PHI (e.g. resident health information) must be kept confidential and only be accessed by authorized users.

Secure Practices for LTCHomes.net users

- Tell your Home Administrator and MOHLTC Nursing Inspector if you think Portal information may have been compromised.
- Log-off the Portal when you are finished using it.
- Do not access the Portal from public computers.
- Do not attach documents or emails to Portal applications if you are not certain of the source.
- Do not open emails which you suspect as being spam.
- Do not readily click on links in emails from unknown sources.
- Be aware of Phishing (attempts to acquire a username, password by masquerading as a trustworthy entity in an electronic communication).
- Be aware of social engineering (use of deception and manipulation to obtain confidential information). Examples include:
  - An individual distracting an authorized user to gain access to a password made visible near a person’s workstation.
  - An individual contacting an authorized user by phone pretending to be a new employee needing an account or technical support staff needing the user’s account information.

Password Security

- Do not share user account information with others or reveal your password to anyone, even if they say there is a good reason. This includes co-workers and supervisors. Your IT department should generally not require your password.
- Avoid writing passwords down. If you need to write it down, store the paper in a locked cabinet rather than posted on your monitor, under your keyboard, or in a drawer near your computer. A better option is to use a phrase to help you remember your password.
- Change your password if you think it has been compromised and choose one that would not be easy for others to guess (name, telephone number, birth date etc.)
- Use different passwords for different website accounts. At a minimum, use a different password for less sensitive accounts than for more sensitive accounts. Also use different passwords for work and non-work accounts.
- Avoid storing passwords that provide access to sensitive information on mobile devices unless the devices are encrypted with a password.
User Account Management

- If you are the home’s User Account Manager (UAM), do not set up a generic account for multiple staff to use.
- UAMs should not send password resets via email. When resetting a password for a user, contact them on the phone or tell them the password in person.
- UAMs are responsible for inactivating user accounts when staff leaves the organization.
- Assign a primary UAM and a back-up. In the event the UAM leaves the organization, the other UAM can inactivate their account and set up a replacement.
- Whenever possible, users should avoid using “freemail” accounts, such as Hotmail, Gmail and Rogers as their registered email address on the Portal.

Workstation Security

- Ensure all computers and networks used to access the Portal have up-to-date virus and spyware/malware protection.
- Set up your workstation so that unauthorized people and passers-by cannot see sensitive information on your monitor.
- When replacing computers, ensure all data is 100% removed prior to disposal (use special software or consult an IT professional prior to disposal)