Secure Messaging Service User Guide

What is the purpose of the secure messaging system?

The secure messaging system enables Canada Life auditors to submit electronic audit requests on paramedical (Extended Health Care [EHC]) claims submitted for PSHCP plan members directly to providers in a secure, electronic format. This new feature promotes regulatory compliance and enhances the audit process. Auditors may initiate audit requests and providers will be able to respond to requests via the secure messaging system located in the Provider Portal.

What is the process for completing an audit?

- When Canada Life initiates an audit request for a paramedical (EHC) claim, it may require additional information to support the audit. If additional information is required from a provider, or an auditor needs to generate a message to a provider, the auditor logs into the secure messaging system and completes an audit request.
- The secure messaging system emails this request to the provider, advising them to log into the application via the Provider Portal.
- The provider logs in and views the audit request (noted by a case number), then follows the audit instructions, which include uploading required supporting documentation, and then replies to the auditor.
- The auditor reviews the attachments and comments and either closes the request, or initiates a follow-up request if more information is required.

Who uses the secure messaging system?

Currently, the secure messaging system is used by Canada Life auditors and paramedical (EHC) providers to manage audits on claims for PSHCP plan members. The **Audit requests** link in the Provider Portal is visible only to user administrators.

Is the secure messaging system available only to providers who have submitted PSHCP claims?

Yes. At this time, the secure messaging system is available only for PSHCP providers who Canada Life auditors have asked to provide additional documentation in response to an audit request or notice. We are looking to expand this service to other insurers in the future.

How will a provider know that an audit request or notice request has been assigned to them?

Providers will receive an email notification when an audit and notice request is assigned to them.

What types of documents can providers upload?

Providers can upload documents that have the following file extensions: JPG, JPEG, TIFF, PNG, BMP or PDF.

What do the statuses in the secure messaging system signify?

The following table describes all of the statuses of the secure messaging system.

Status	Description
New	The provider has not yet viewed the case.
Open	The request has been viewed by the provider, but they have yet to submit the information requested to the auditor.

Status	Description
Follow Up Requested	The auditor has contacted the provider to remind them to act on the request, because the information the provider sent is insufficient to make a proper decision on the request, or because the due date changed.
In progress	The provider has added a comment to the case or uploaded a file but not yet submitted it.
Submitted	The provider has submitted a response to the request.
Closed	The auditor has closed the request; no additional actions are required.

Who should providers reach out to if they have a question about an audit or notice request?

Please do one of the following:

- log into the secure messaging system, select the case that is associated with the Audit ID, and leave a message for the auditor, or
- contact Canada Life directly at: 1-855-415-4414, Monday to Friday 8 a.m. to 5 p.m. caller's local time.

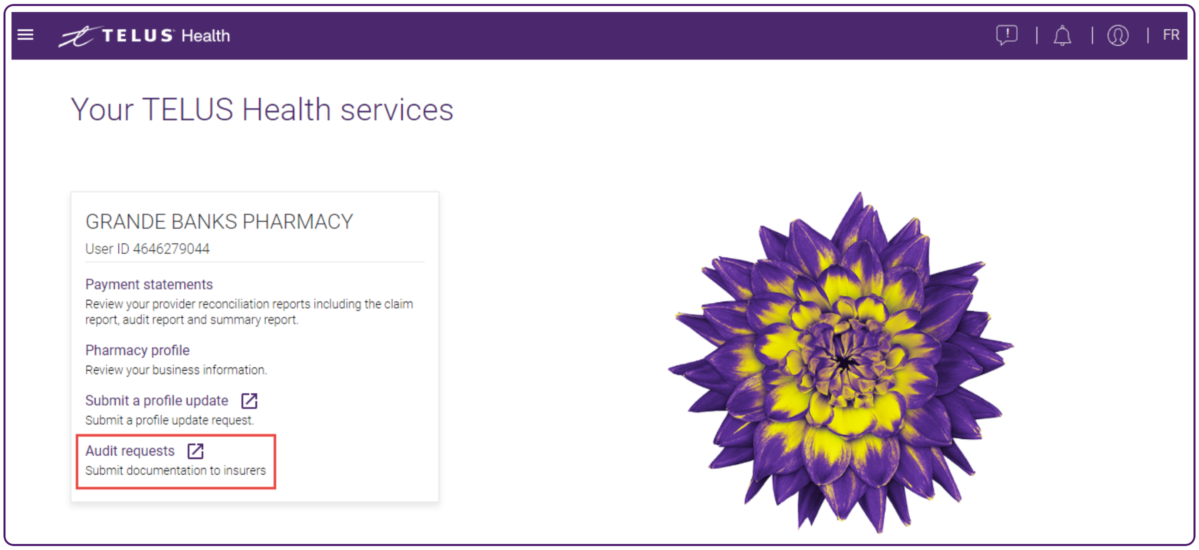
Who should users contact if they are experiencing issues with the secure messaging system?

- Providers should call the eClaims IVR #: 1-866-240-7492, and select option 4 to reach the PMG Service Desk.
- Auditors should call the Carrier IVR at 1-866-342-6570. The CE Tier2IM Service Desk will start the incident management process.

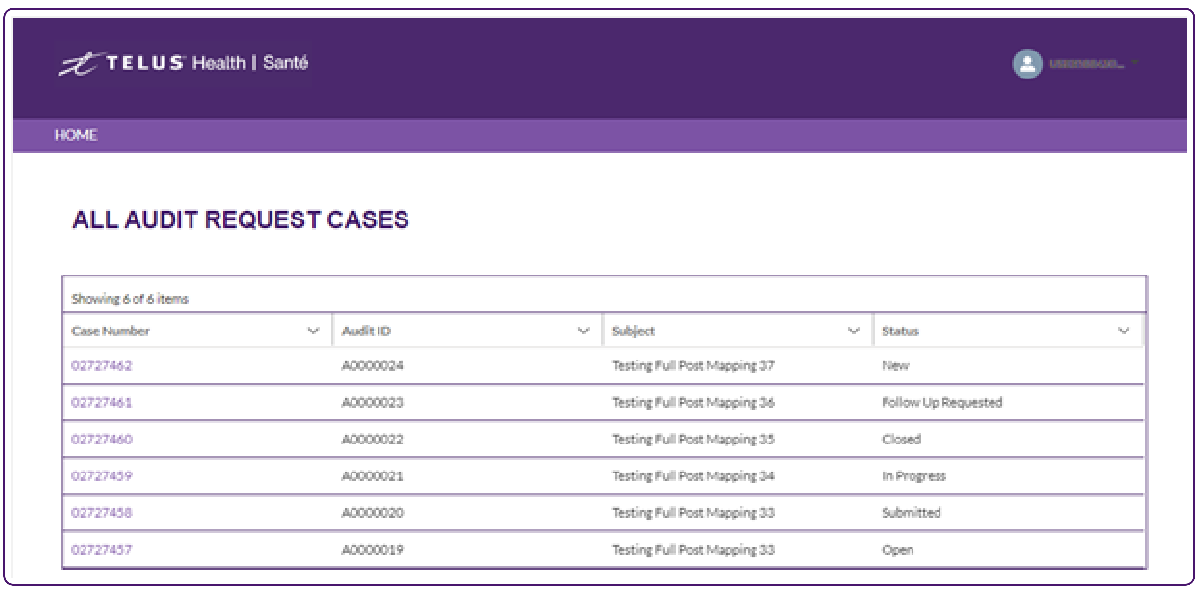
Responding to audit requests

The following procedure describes how you, as an EHC provider, can respond to your audit requests.

1. Log into the Provider portal.
2. From the TELUS Health services page, select the **Audit requests** link.

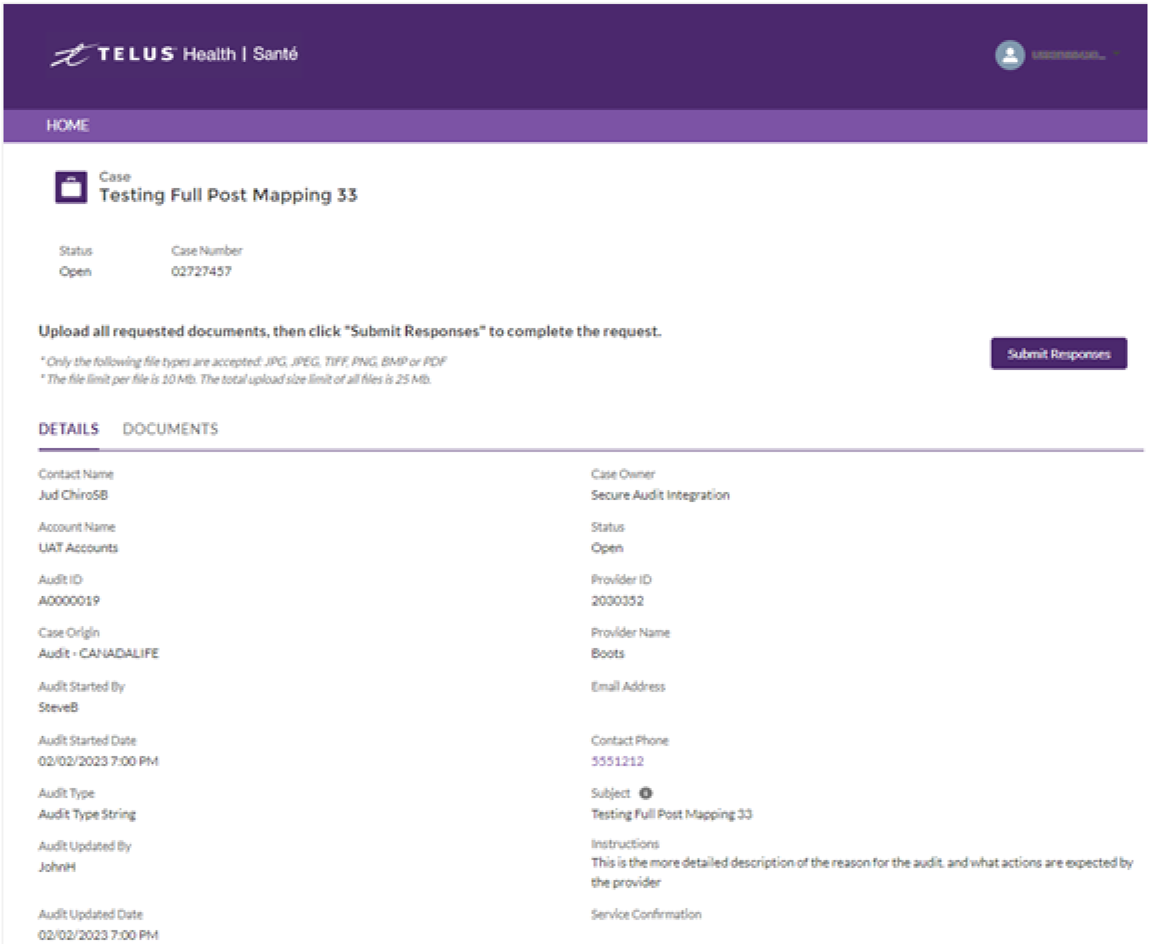


The audit requests page is displayed.



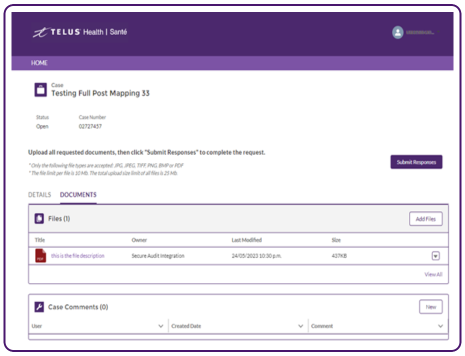
3. Select the case number of the request you want to view.

   The **Case** page is displayed.



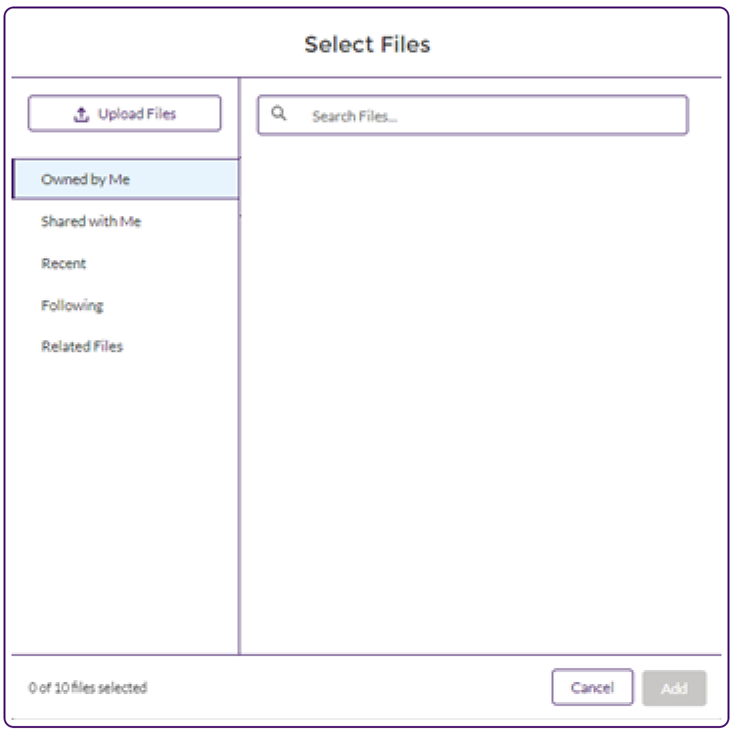
4. To add documents to the request:

   - Select the **Documents** tab.

   - Select **Add Files**.

     The **Select Files** pop-up is displayed.

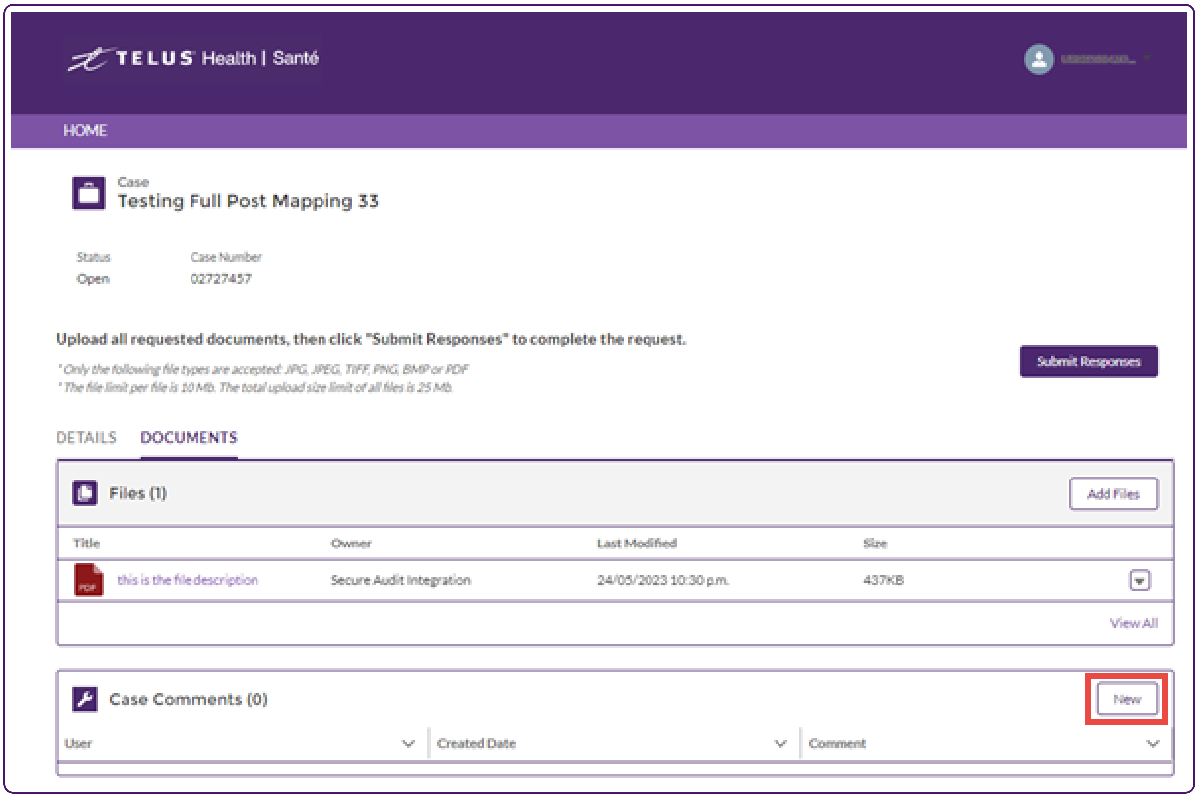
   - Select **Upload Files**.
   - Locate and select the file you want to upload, then select **Open** and **Done**.

     After the file has been uploaded, it is displayed in the **Files** section of the **Documents** tab.

   - To verify the document, double click the name of the file to open it in a new tab, or select the Download button to its right.

5. To add comments to the request:

   - On the **Details** tab, scroll down to the **Comment** section, and select **New**.



The **Case Comments** pop-up is displayed.

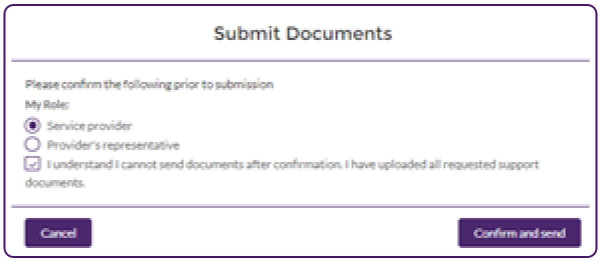
   - Enter your comments and then select **Add**.

You can add up to 4000 characters.

You cannot delete or modify comments once they have been saved.

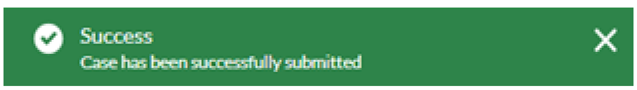
6. To submit a response:
   - Select **Send documents**.

     The **Submit Documents** pop-up is displayed.

   - Select your appropriate role, then select the check box next to the confirmation statement.
   - Select **Confirm and send**.

     The following confirmation message is displayed.

     The **Status** of the audit request on the **Case** page changes to Submitted.

