

Set Up Shared Encryption Key

This guide explains how to create, save, view, and reset the Shared Encryption Key (SEK). It is intended primarily for **Ocean Site Admins**. General users only need to refer to **Step 4: Enter the SEK – OPTION 2: General User: Enter SEK on eReferrals & eConsults page**; all other content is intended for Ocean Site Admins.

Purpose of the SEK

The SEK is a private encryption key that allows Ocean sites to securely view and exchange patient information. It may need to be entered when a new user joins an Ocean site or when eReferrals is accessed from a new device or browser.

The SEK should only be shared with users who are authorized to access private patient data.

Important Notes:

- Saving the SEK to [Ocean Cloud Connect](#) is mandatory for the DRO eReferrals program.
- For privacy and security, **the SEK cannot be retrieved by the DRO Team**. If access is lost, the key can only be reset by Ocean upon request from a Site Admin.
- **Resetting the SEK may result in the loss of data associated with previous eReferrals.**
- Only an Ocean Site Admin can create, save, view, and reset the SEK.

To ensure continuous access to the SEK:

- Have at least two Site Admins at your Ocean site.
- Ensure all Site Admins [enter the SEK into the Encryption section](#) of their Ocean account.
- Complete and securely store the [Clinic Reference Card](#) on-site.

Contents

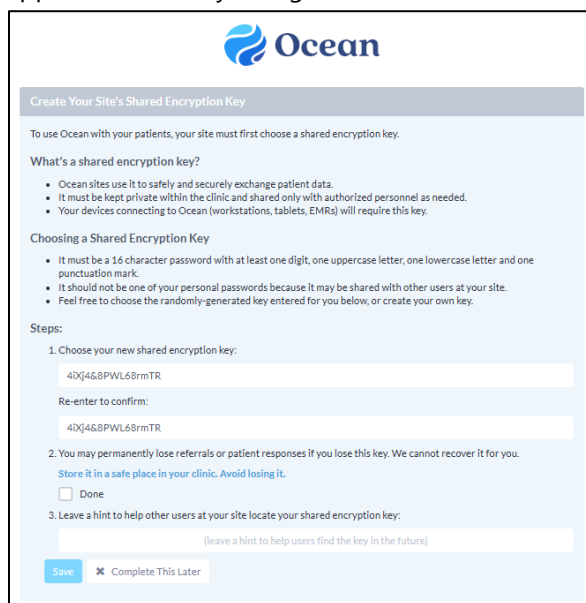
Step 1: Create the SEK.....	2
Step 2: Save the SEK to Ocean Cloud Connect.....	5
Step 3: View the SEK.....	6
Step 4: Enter the SEK	8
OPTION 1: Site Admin: Enter SEK on Encryption page	8
OPTION 2: General User: Enter SEK on eReferrals & eConsults page.....	9
Step 5: Reset the SEK.....	10

Step 1: Create the SEK

Note: This step only applies to Ocean Site Admins.

Warning: Follow these instructions carefully. Do not save the SEK until directed. Saving it early may require a reset by the Ocean team and delay the process.

1. Log in to [Ocean](#).
2. When the SEK has not been created, the **Create Your Site's Shared Encryption Key** screen may appear whenever you log into Ocean.



Create Your Site's Shared Encryption Key

To use Ocean with your patients, your site must first choose a shared encryption key.

What's a shared encryption key?

- Ocean sites use it to safely and securely exchange patient data.
- It must be kept private within the clinic and shared only with authorized personnel as needed.
- Your devices connecting to Ocean (workstations, tablets, EMRs) will require this key.

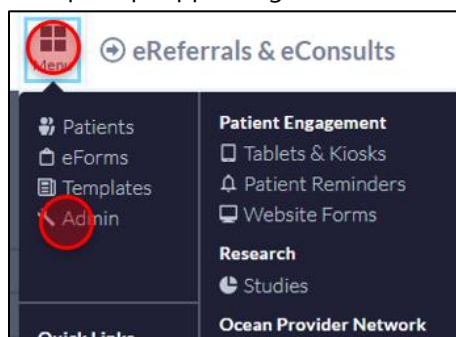
Choosing a Shared Encryption Key

- It must be a 16 character password with at least one digit, one uppercase letter, one lowercase letter and one punctuation mark.
- It should not be one of your personal passwords because it may be shared with other users at your site.
- Feel free to choose the randomly-generated key entered for you below, or create your own key.

Steps:

1. Choose your new shared encryption key:
- Re-enter to confirm:
2. You may permanently lose referrals or patient responses if you lose this key. We cannot recover it for you.
 Store it in a safe place in your clinic. Avoid losing it.
☐ Done
3. Leave a hint to help other users at your site locate your shared encryption key:

3. If no prompt appears, go to **Menu > Admin > Encryption** to create one manually.



Menu Admin Settings

Admin Settings

Site Settings

Site Account
View and configure basic information about your account, including notification emails and timezone.

Encryption
Set up or view your site's shared encryption key.

Users
Invite and manage users at your site.

Licence Management

4. On the **Create Your Site's Shared Encryption Key** screen, complete the three steps. **Do not click Save until directed.**

Create Your Site's Shared Encryption Key

To use Ocean with your patients, your site must first choose a shared encryption key.

What's a shared encryption key?

- Ocean sites use it to safely and securely exchange patient data.
- It must be kept private within the clinic and shared only with authorized personnel as needed.
- Your devices connecting to Ocean (workstations, tablets, EMRs) will require this key.

Choosing a Shared Encryption Key

- It must be a 16 character password with at least one digit, one uppercase letter, one lowercase letter and one punctuation mark.
- It should not be one of your personal passwords because it may be shared with other users at your site.
- Feel free to choose the randomly-generated key entered for you below, or create your own key.

Steps:

1. Choose your new shared encryption key:
 98V4zSzWhABFgJ
 Re-enter to confirm:
 98V4zSzWhABFgJ
2. You may permanently lose referrals or patient responses if you lose this key. We cannot recover it for you.
[Store it in a safe place in your clinic. Avoid losing it.](#)
☐ Done
3. Leave a hint to help other users at your site locate your shared encryption key:
 (leave a hint to help users find the key in the future)

Save

DO NOT CLICK SAVE!

- Choose a new Shared Encryption Key.**
 - A key is generated automatically. While you may create your own, the generated key is recommended for stronger security.
 - The key must be 16 characters long.
 - It must contain at least:
 - one digit
 - one uppercase letter
 - one lowercase letter

4. one punctuation mark (e.g. !, ,, _ , @, etc.).
 - iv. Do not use a personal password as the SEK may need to be shared with other authorized users at your site.
 - b. Select the **Done** checkbox to confirm that you understand the risk of losing access to previous referral data if the SEK is lost, and that you will maintain an on-site back up.
 - c. Enter a hint indicating where the SEK can be found at your site.
 - d. **Do not click Save yet.**
5. Download the [Clinic Reference Card](#).
 - a. Complete the reference card, ensuring the SEK is accurately recorded.
 - b. Save the completed reference card to your computer.
 - c. Ensure the hint entered above directs authorized users to the location of the reference card or to a Site Admin who has access to the SEK.
 - d. Keep the reference card open. You will need the SEK again in **Step 2: Save the SEK to Ocean Cloud Connect**.
6. **Confirm the following before clicking Save:**
 - a. **The SEK has been entered correctly on the reference card.**
 - b. **The completed reference card has been securely saved.**
7. Click **Save**.

35Yoz@PdFuSpu43L

Re-enter to confirm:

35Yoz@PdFuSpu43L

2. You may permanently lose referrals or patient responses if you lose this key. We ca

Store it in a safe place in your clinic. Avoid losing it.

☒ Done

3. Leave a hint to help other users at your site locate your shared encryption key:

In the main filing cabinet

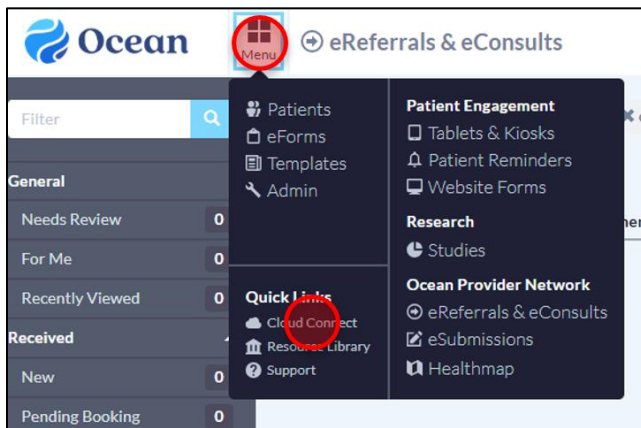
Save Complete This Later

Step 2: Save the SEK to Ocean Cloud Connect

Note: This step only applies to Ocean Site Admins.

Saving the SEK to Cloud Connect is a mandatory program requirement, as it is the only way to reset the SEK if it is lost or cannot be retrieved.

1. Go to **Menu > Cloud Connect**

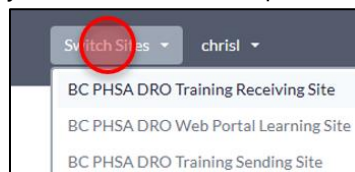


2. You will be prompted to sign into **Ocean Cloud Connect**. Enter your Ocean username and password and click **Secure Sign In**.

3. The site that is selected will be displayed at the top.



- a. If you belong to multiple Ocean Sites, click **Switch Sites** in the top-right corner and select your site from the drop-down menu.



4. Click **Store my Encryption Key**.

Welcome to Ocean Cloud Connect

Ocean Cloud Connect is a secure integration server that can connect your Ocean site with your EMR.

If you use a partner EMR that provides a supported Application Programming Interface (API), Cloud Connect can securely transfer patient data between your systems, enabling you to access powerful Ocean features right from your EMR. Cloud Connect will request that you enter your site's Shared Encryption Key in order to encrypt sensitive data before it is transferred to Ocean.

To connect your EMR with Ocean, click 'Integrate with my EMR' and follow the steps.

Alternatively, you can use Cloud Connect to securely store your Shared Encryption Key without configuring an EMR. Once stored, you can log into Cloud Connect to retrieve your Shared Encryption Key and authorize additional tablets or web browsers.

Integrate with my EMR Store my Encryption Key

5. Enter the SEK, then click **Save**.

Store Shared Encryption Key

Please enter your site's Shared Encryption Key. Your Shared Encryption Key is the 16-character key you created in the Admin tab of the Ocean Portal.

For more information, [click here](#).

Shared Encryption Key 7uWSEk1LjPd<1Jt8

Cancel Save

6. This saves your SEK to Ocean Cloud Connect, which creates a digital backup that can be used to support future reset requests if needed.
7. Before using Ocean Cloud Connect, consult the Clinic Reference Card or contact a Site Admin with access to the SEK. Site Admins can view the SEK at any time by following **Step 3: View the SEK**.

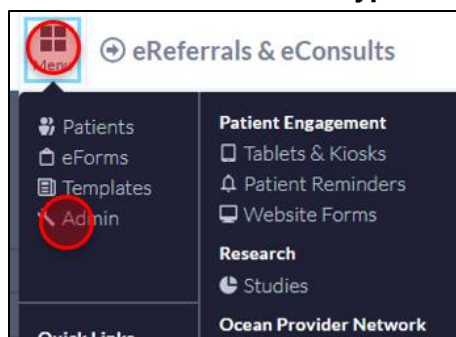
Step 3: View the SEK

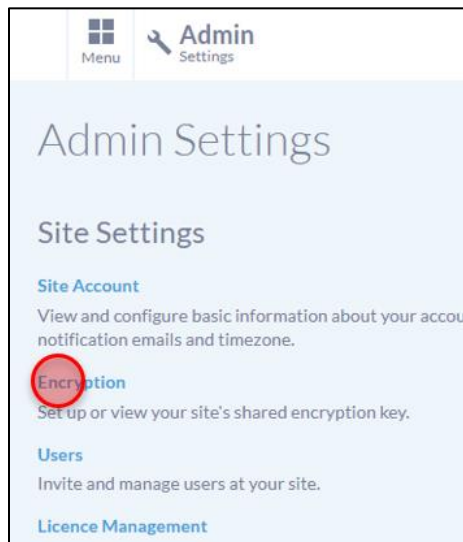
Note: This step only applies to Ocean Site Admins.

The SEK is automatically saved and can be viewed by your site's initial Site Admin.

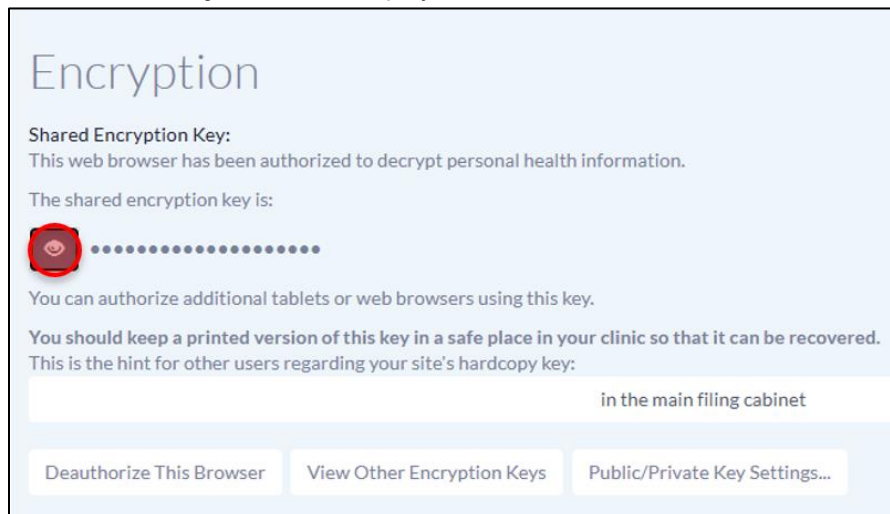
It is only visible to other Site Admins after they enter it (see **Step 4: Enter the SEK**). Once entered, they can view and share it with other authorized users.

1. Go to **Menu > Admin > Encryption**.





2. Click the **visibility button** to display the SEK.



3. The SEK may be shared with authorized users who access private patient data and support your site's eReferral workflow.

Step 4: Enter the SEK

The SEK should be entered by all Site Admins to ensure that it is securely backed up across multiple accounts and remains accessible when needed.

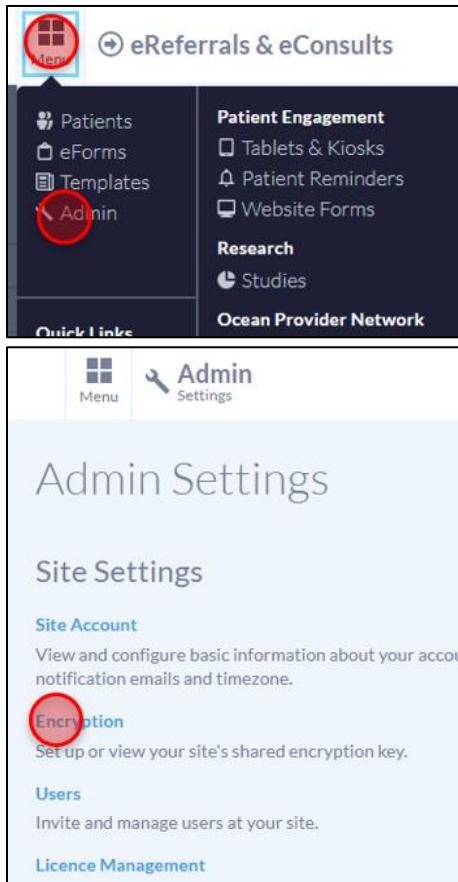
It should also be entered by all authorized users who access private patient data and support your site's eReferral workflow.

The SEK must be entered each time a new device or browser is used.

OPTION 1: Site Admin: Enter SEK on Encryption page

Note: This option only applies to Ocean Site Admins.

1. After a Site Admin shares the SEK, go to **Menu > Admin > Encryption**.



2. Enter the SEK into the field and click **Enter**.

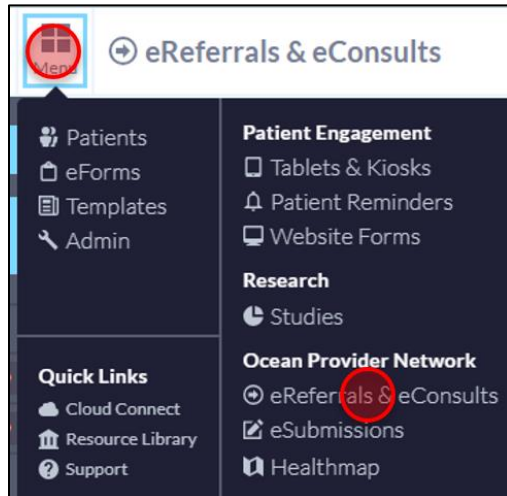
The screenshot shows the 'Encryption' page. The title 'Encryption' is at the top. Below it, the text reads: 'Enter Your Shared Encryption Key: This web browser is not yet authorized to decrypt personal health information: To authorize this browser, you must enter your site's shared encryption key:'. There is a text input field for the 'Enter shared encryption key'. Below the field, there is a paragraph: 'Your shared encryption key is shared among the Ocean users at your site. If you are not sure what your key is, please check with your Ocean site administrator. Here is a hint left by your site to help you locate it: in the main filing cabinet You can also check any browser in your clinic that is pre-authorized with the shared encryption key. For your reference, the key was created by chrisl (Chris Lee) on Jun 26, 2026.' At the bottom right, there is a red 'Enter' button.

3. The SEK is saved and can be viewed by returning to this page.

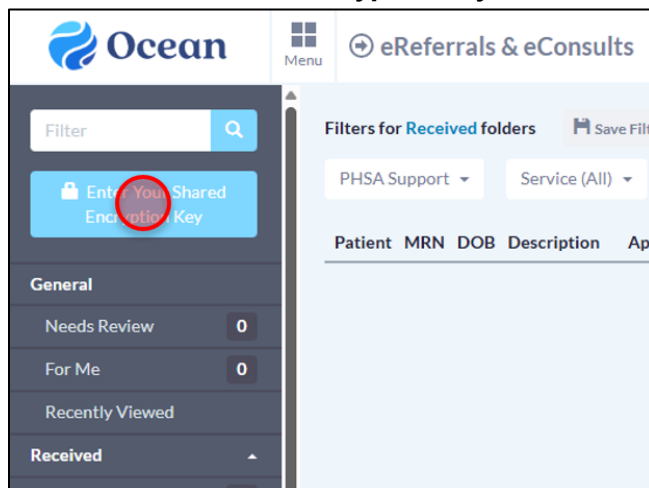
OPTION 2: General User: Enter SEK on eReferrals & eConsults page

General users must enter the SEK to view eReferral patient information.

1. After a Site Admin shares the SEK, go to **Menu > Admin > eReferrals & eConsults**



2. Click **Enter Your Shared Encryption Key.**



3. Enter the SEK into the field and click **Enter.**

Encryption

Enter Your Shared Encryption Key:
 This web browser is not yet authorized to decrypt personal health information:
 To authorize this browser, you must enter your site's shared encryption key:

Your shared encryption key is shared among the Ocean users at your site.
 If you are not sure what your key is, please check with your Ocean site administrator.
 Here is a hint left by your site to help you locate it:
in the main filing cabinet
 You can also check any browser in your clinic that is pre-authorized with the shared encryption key.
 For your reference, the key was created by chrisl (Chris Lee) on Jun 26, 2026.

Enter

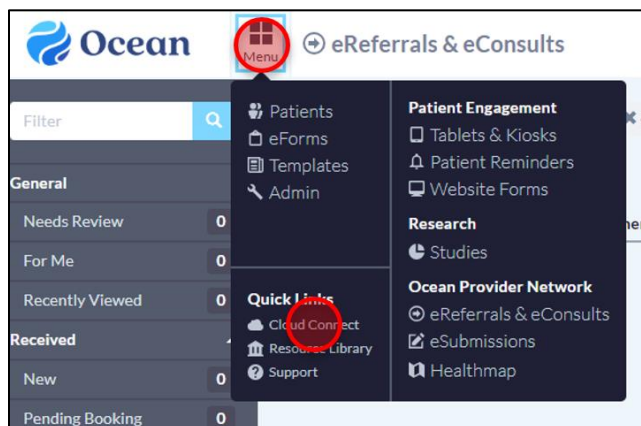
Step 5: Reset the SEK

Note: This step only applies to Ocean Site Admins.

Before resetting the SEK, follow **Step 3: View the SEK** or retrieve your on-site backup (e.g., your site's Clinic Reference Card).

For privacy and security, the SEK cannot be retrieved by the DRO Team. If access is lost, the key can only be reset by Ocean upon request from a Site Admin.

1. Go to **Menu > Cloud Connect**



2. You will be prompted to sign into Ocean Cloud Connect. Enter your Ocean username and password and click **Secure Sign In**.



Ocean Cloud Connect

Ocean Cloud Connect Sign In

Two-factor authentication must be enabled on your Ocean user account to access Cloud Connect.

[Learn more about enabling two-factor authentication here.](#)

User Name
username

Password
.....

[Forgot Ocean User Name?](#)

[Forgot Ocean Password?](#)

☒ Remember me on this computer

[Secure Site Sign In](#) [Looking for the Ocean Portal? Sign In here!](#)

3. The site that is selected will be displayed at the top.

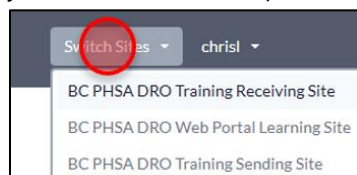


Ocean Cloud Connect **BC PHSA DRO Training Receiving Site (19403)**

[Switch Sites](#) [chrisl](#)

- BC PHSA DRO Training Receiving Site
- BC PHSA DRO Web Portal Learning Site
- BC PHSA DRO Training Sending Site

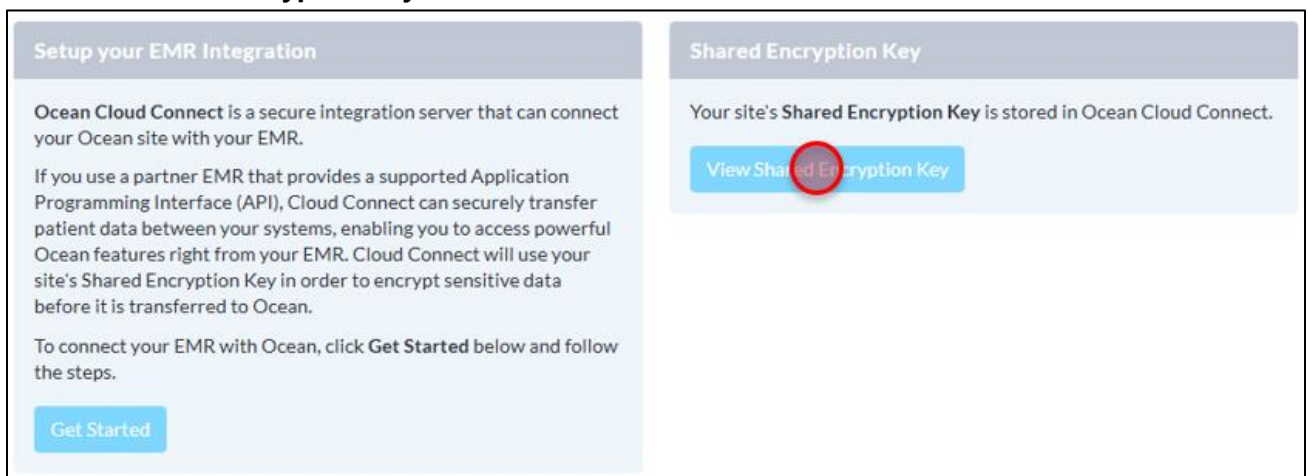
- a. If you belong to multiple Ocean Sites, click **Switch Sites** in the top-right corner and select your site from the drop-down menu.



[Switch Sites](#) [chrisl](#)

- BC PHSA DRO Training Receiving Site
- BC PHSA DRO Web Portal Learning Site
- BC PHSA DRO Training Sending Site

3. Click **View Shared Encryption Key**.



Setup your EMR Integration

Ocean Cloud Connect is a secure integration server that can connect your Ocean site with your EMR.

If you use a partner EMR that provides a supported Application Programming Interface (API), Cloud Connect can securely transfer patient data between your systems, enabling you to access powerful Ocean features right from your EMR. Cloud Connect will use your site's Shared Encryption Key in order to encrypt sensitive data before it is transferred to Ocean.

To connect your EMR with Ocean, click **Get Started** below and follow the steps.

[Get Started](#)

Shared Encryption Key

Your site's Shared Encryption Key is stored in Ocean Cloud Connect.

[View Shared Encryption Key](#)

4. Click on **Shared Encryption Key Emergency Access Form** to submit a request.

View Shared Encryption Key

Please try the [other methods to retrieve your Shared Encryption Key](#) before using this option.

If you still need access, submit a request through the [Shared Encryption Key Emergency Access Form](#). An OceanMD Support Team member will verify your identity and provide a permission code. Enter the code below to view the key.

Viewing the key will send an email notification to your site's Clinical Administrator.

Permission Code

Cancel

View Shared Encryption Key

5. The Ocean team will contact you with further instructions.

Questions?

If you have questions or require assistance with creating your Directory Listing, please contact the Digital Referrals and Orders team: dro.program@phsa.ca.