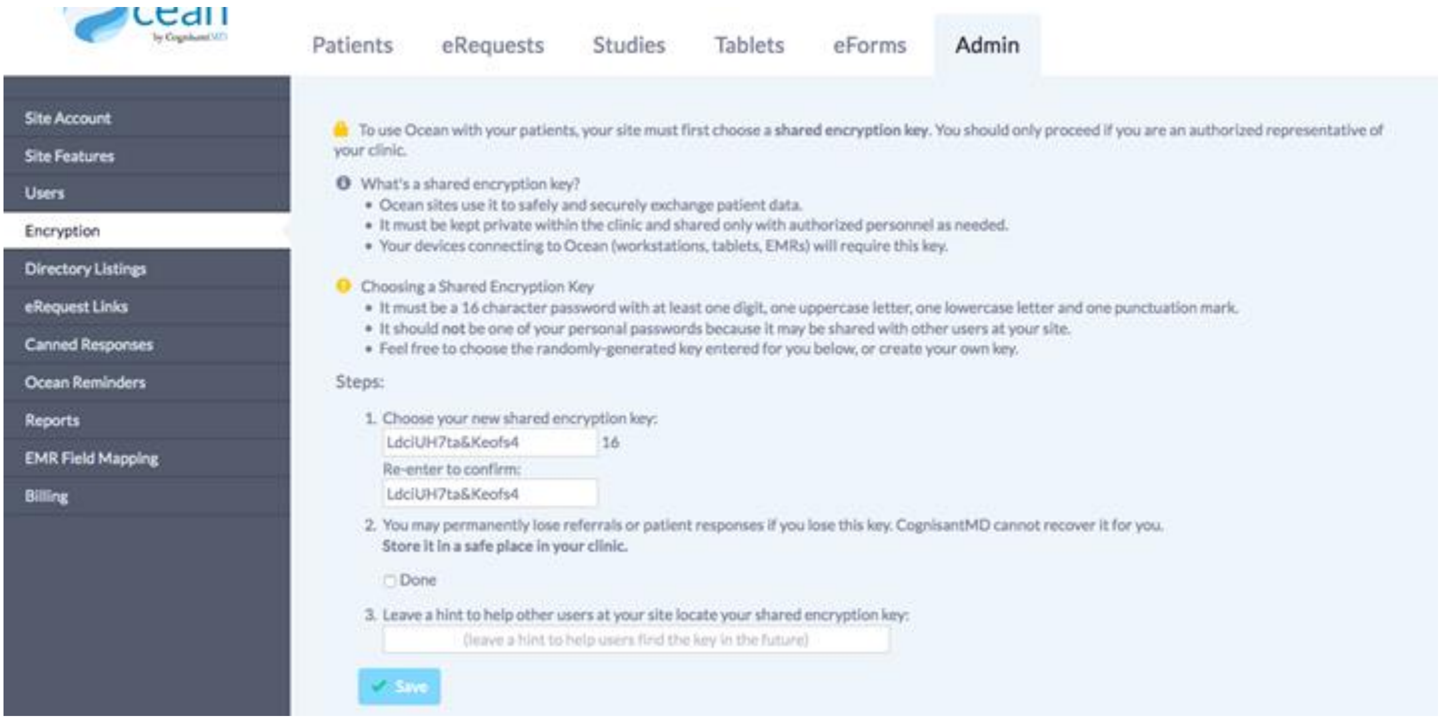
Instructions to create a new Shared Encryption Key are as follows:

- The new Shared Encryption Key will need to be entered into the browser on **each** workstation that will be used in order to view the referral information.
- The information needed to set up your new shared encryption key can be found within Ocean by clicking the support button on the ”Home” screen and performing a search or by following:

  https://cognisantmd.zendesk.com/hc/en-us/articles/115001651312-The-Shared-Encryption-Key

Setting Up Your Shared Encryption Key

- Log in to the Ocean Portal and navigate to the Admin tab
- Enter the "**Encryption**" section (selected from the menu on the left) to set up your shared encryption key. You may choose to either type in a shared encryption key of your choice or keep the auto-generated key.



To use Ocean with your patients, your site must first choose a **shared encryption key**. You should only proceed if you are an authorized representative of your clinic.

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:
   LdciUH7ta&Keofs4 16
   Re-enter to confirm:
   LdciUH7ta&Keofs4
2. You may permanently lose referrals or patient responses if you lose this key. CognisantMD cannot recover it for you.
   Store it in a safe place in your clinic.

   □ 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

Requirements for the Shared Encryption Key:

- It must be 16-characters with at least one digit, one uppercase letter, one lowercase letter and one punctuation mark (e.g !,.,_,@,etc.)
- It should **NOT** be one of your personal passwords because it will be shared with other users at your site.
- Feel free to choose the randomly generated key that is generated for your site automatically or create your own key.
- You must acknowledge that you’ve stored your shared encryption key in a safe spot (step 2) and left a hint (step 3) in case you need to enter your encryption key again in the future (e.g. if you get a new computer or use a new browser).
- Click “Save” to save your shared encryption key.
- You can return to this “Encryption” section of the Admin tab to view your shared encryption key at any time.

<u>Important Notes about the Shared Encryption Key</u>

Your shared encryption key is the ultimate guard against unauthorized access to your patient's data, and should therefore be handled with great care and stored in a safe place. For safekeeping, we recommend that you download, print, and complete this Clinic Reference Card and keep it in a safe location for future reference.

It’s also recommended that access to the key be limited to trusted administrative account holders.

If you have misplaced your encryption key, try following the steps outlined in "Recovering a Lost / Forgotten Shared Encryption Key" to recover it.

In the worst case scenario where your encryption key really has been lost, CognisantMD will NOT be able to find or retrieve your unique key on your behalf (this is one of the ways we help to ensure patient data is always secure).