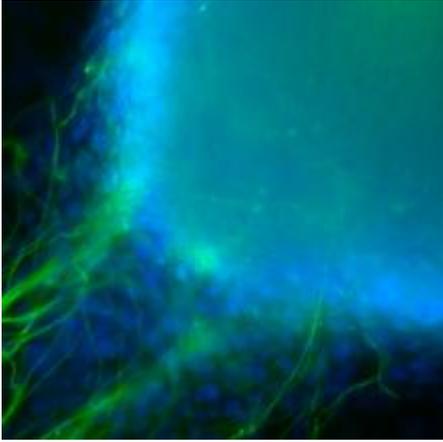


Secure Box (CipherCloud)



Dejon Lewis on January 31, 2020

Overview



Secure Box allows UCSF Box users to store restricted data, while protecting UCSF and our patients, staff, and students from data loss.

Please note that we are only scanning for UCSF PHI; we are not scanning multimedia formats (image, video, audio files, scanned PDFs) or files over 400MB.

We launched CipherCloud on **Monday, October 3, 2016.**

In **November 2016**, we will begin scanning files that were already on Box at Secure Box launch time. This process will take months to complete, so UCSF Box users may see older files encrypted months after the launch.

What Is Secure Box?

With the implementation of CipherCloud UCSF Box users will see the following changes.

Secure Folder

Each UCSF Box user gets a secure folder. UCSF Box users can use this folder to store any files they want, but restricted data *must* be stored in the secure folder. Non-UCSF collaborators cannot access the secure folder. All files in the secure folder are encrypted, and a very lightweight CipherCloud agent is required to open these files.

Scanning for PHI from APeX

The initial phase of CipherCloud scanning targets PHI from APeX, using the same rules as our email data loss prevention tool. When PHI is detected the file is encrypted in place, and a PDF "marker file" of the same name as the encrypted file is placed in the folder explaining what actions were taken. After the file is encrypted the CipherCloud agent is required to open file. Non-UCSF collaborators will not be able to open these encrypted files.

Resources

Software

Desktop Agents

Desktop agents are pushed to all computers supported by UCSF IT, but you can also download the software from the UCSF software website. To find the CipherCloud agents on the software website:

1. Go to <https://software.ucsf.edu> [1] and login via MyAccess
2. Click on Other Software, or search for 'CipherCloud'

Mobile Apps

The CipherCloud mobile app is available for iOS (iPhone and iPad) and Android, and requires the Box app to function.

- iOS (iPhone and iPad) ? from the iTunes app store
 - Box app [2]
 - CipherCloud app [3]
- Android ? from Google Play
 - Box app [4]
 - CipherCloud for Box app [5] ? *note: only this version works with Box*

Training & Support

-  Secure Box Information slides (PDF) [6]
-  UCSF CipherCloud Agent Install and User Guide (PDF) [7]

Support is handled through the UCSF IT Service Desk [8].

FAQ

1.

How does CipherCloud work?

- CipherCloud scans files for restricted data when they are uploaded to Box. If a file contains PHI from a UCSF patient then it is encrypted, and can only be read using the CipherCloud agent. When you attempt to open an encrypted file, the CipherCloud agent on your system will log you in to Box and retrieve the encryption key from the CipherCloud server, making the document completely accessible to you. Encryption keys last 30 days, after which time you must have an internet connection and a UCSF Box login to decrypt a .ccsecure file.

2.

What kinds of data are we scanning for?

- UCSF's data loss prevention (DLP) system, which is the scanning engine used to scan outbound emails and Box content, is currently configured to scan for PHI that matches UCSF patient records in APeX. Today we are not scanning for PHI from UCSF Dentistry, BCHO, or ZSFG medical records, but we may at some time in the future. We are also not scanning multimedia file formats (images, video, audio, scanned PDFs), so please store any multimedia files containing restricted data in your secure folder. We are currently not scanning files over 400MB, so it's important that you put files with restricted data regardless of size in the secure folder.

3.

How are we identifying UCSF PHI?

- When CipherCloud detects a change to a file (new file upload, a file edit, change to collaborators) CipherCloud sends this data to the DLP system, which will scan the data for matches to UCSF's patient record index from APeX.

4.

What kinds of data can and can't be put in the secure folder?

- The secure folder on Box will encrypt *any* data placed into that folder or subfolder. This ensures that all types of restricted data will be protected.

5.

When should I use secure folder?

- Use the secure folder for anything, but note that items in the Secure folder cannot be shared outside of UCSF. Also keep in mind that you can't preview encrypted files.

6.

When should I *not* use secure folder?

- You should not use the secure folder when you want to share files with someone

outside of UCSF. In addition, there are some uses for which Box is not a good solution. Please see the UCSF Box FAQ [9] for more information.

7.

What happens when you find UCSF PHI outside of the secure folder?

- The file that contains UCSF PHI will be encrypted, and can only be viewed from devices with the CipherCloud agent. Any external collaborators in the folder will not be able to access the file. Because of the CipherCloud encryption, you will not be able to preview the file within Box. There will also be a marker file, with a message explaining that the file has been encrypted because it has UCSF PHI and explains the steps to view it.

8.

How long does encryption/decryption take on UCSF Box?

- The background process that scans for UCSF PHI and encrypts files when it is found, or decrypts files when it is removed, takes anywhere from 30 seconds to several minutes. If a file has not been encrypted/decrypted after 5 minutes please contact the IT Service Desk.
- Files opened on your computer with the CipherCloud agent should decrypt and encrypt in less than 15 seconds.

9.

You already told us not to use Box for restricted data. How has that changed?

- **Effective October 3, 2016** you can store restricted data (e.g., PHI, PII, PCI, FERPA) in the Box secure folder. If you need to share restricted data with non-UCSF collaborators please use MyResearch [10].

10.

Is there a performance hit using the agent?

- When the agent isn't actively encrypting or decrypting a file there is no performance difference. During decryption and encryption there is a very small delay, the length of which depends on the size of the file.

11.

How is the agent updated?

- The CipherCloud agent is distributed and updated by BigFix, or it can be downloaded from the <https://software.ucsf.edu> [1].

12.

Is there end-user training?

- Please see the UCSF CipherCloud Agent Install and User Guide [7].

13.

I'm an IT partner. Is there a Secure Box KnowledgeBase article in ServiceNow?

- Yes, see KB0018087 [11], or search for *CipherCloud* or *Secure Box*.

14.

You blocked my collaborator! Now what?!

- CipherCloud encrypts files containing UCSF PHI from UCSF's electronic medical record. Once encrypted, only UCSF users with access to the folder can decrypt the files. Box is not approved for sharing restricted information with collaborators outside of UCSF.

15.

What are my options if I need to share restricted data with a collaborator?

- MyResearch ^[10] is designed to support multi-site studies that involve non-UCSF collaborators. We are able to address researchers' questions about the use of MyResearch for multi-site studies and about sharing data with non-UCSF collaborators. Please email its-arssupport@ucsf.edu ^[12] with any questions you may have.
- Another option is to sponsor your collaborator as an affiliate, so they can use a UCSF login, then they will be treated as a UCSF user. A discounted Data Network Recharge rate applies to affiliates. See the Data Network Recharge: FAQ ^[13] for more information.

16.

What happens if I try to open an encrypted file via the Box website or using a third-party Box application?

- Box Preview will not work with a .ccsecure encrypted file. Box will display a message that reads "We're sorry, but we can't preview .ccsecure files." You can use Box Edit or download the file to your computer with the CipherCloud agent or open it on your mobile device with the CipherCloud app to view it.

17.

I don't store UCSF PHI on Box. Why was my file encrypted?

- Many people don't realize they have UCSF PHI, which is one reason it's so important to use a tool like CipherCloud. For more information about what PHI is and isn't, and your responsibilities when handling it, please refer to the UCSF Privacy Office's Workforce Resources and Guidance page ^[14].

18.

Can I edit encrypted files on my mobile device?

- You can access encrypted files on your mobile device as long as you have the CipherCloud app installed. To edit a file once CipherCloud has opened it, use the "open in" icon in the lower left to select an application which can open the file for editing. *Please note, this will put an unencrypted copy of the file on your mobile device.* As with all mobile applications, your ability to edit the file depends on which apps you have installed. You may only have the option to import or copy a file into an application to edit it, so if you need to make edits we recommend doing this from a computer instead. This will ensure that you are not saving unencrypted copies of restricted data on your mobile device.

19.

What happens if I create a Box Note and add UCSF PHI?

- If you add PHI to a Box Note, the Box Note will be encrypted. When CipherCloud decrypts the Box Note it then passes it back to the application that can open it. The application for Box Notes is the Box web application, which is only able to open Box Notes directly, so you will get an error. The upshot that once PHI is detected in a Box Note it is impossible to open it, and the only thing you can do is revert to the previously version.

Required Service Information

UCSF Box ^[15]

Images



GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

[Site Login](#) [Site Index](#)

[Suggest an IT Improvement](#) | © UC Regents

*//-->

Source URL: <https://it.ucsf.edu/services/ucsf-box/additional/secure-box-ciphercloud>

Links

- [1] <https://software.ucsf.edu>
- [2] <https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8>
- [3] <https://itunes.apple.com/us/app/ciphercloud/id896658857?mt=8>
- [4] <https://play.google.com/store/apps/details?id=com.box.android>
- [5] <https://play.google.com/store/apps/details?id=com.cipher.Shield>
- [6] <https://it.ucsf.edu/sites/it.ucsf.edu/files/securebox-info-20160928.pdf>
- [7] https://it.ucsf.edu/sites/it.ucsf.edu/files/ucsf_ciphercloud_agent_install_and_user_guide.pdf
- [8] <https://it.ucsf.edu/about/teams/ucsf-it-service-desk>
- [9] <https://it.ucsf.edu/services/ucsf-box/box-faq>
- [10] <https://myresearch.ucsf.edu/>
- [11] https://ucsf.service-now.com/kb_view_customer.do?sysparm_article=KB0018087
- [12] <mailto:its-arssupport@ucsf.edu>
- [13] <https://it.ucsf.edu/services/data-network-recharge-system-information/data-network-recharge-faq>
- [14] <https://hipaa.ucsf.edu/workforce-resources-and-guidance>
- [15] <https://it.ucsf.edu/services/ucsf-box>