UChicagoBox for BSD
Updates

• On September 26th, UChicagoBox will be available for all of the BSD

• Will be available for individual Box accounts; group (departmental) folders within BSD will be available at a later date

• Will permit the collaboration and sharing amongst BSD faculty and staff, as well as at the University (within HIPAA guidelines)

• Allows for web access, and syncing files on your computer (though HIPAA considerations must be accounted for)

• Large storage options (multiple terabytes).

An instruction guide has been provided on how to use the system. It is available at http://securitybsd.uchicago.edu/wp-content/uploads/sites/2/2016/09/UChicago-Box-Instructions-for-BSD.pdf

More information can be found at http://securitybsd.uchicago.edu/bsduchicagobox/

• Service is not available for UCMC due to cost restrictions; UCMC collaborators will not be able to participate in using the service
UChicagoBox Risks and Concerns

Though the system meets our HIPAA requirements, the use of the technology increases the likelihood of certain risks. Of particular concern are:

• **Inappropriate or unauthorized sharing of PHI. Examples include:**
  - Employees creating “open access links” to PHI that require no authentication
  - Employees sharing PHI with University collaborators who are not in the OHCA

• **Copying of Restricted information to multiple devices through the use of Box Sync, with some of those devices not being encrypted. Examples include:**
  - Setting up a sync amongst your work laptop, work phone and home computer. The laptop and phone might be encrypted, but in many cases the home computer is not. A theft of the home computer could expose data

• **Malicious access to the Box system due to a compromised account. Examples include:**
  - An employee falling prey to a phishing attack which compromises the users account and password. That account and password can log in to Box.
UChicagoBox/HIPAA Requirements

Users must conduct special care when using the UChicagoBox system for Restricted data, such as patient information or human subject research

• Only authorized users are permitted to have access to Restricted data. Follow your IRB protocols to the letter and be conscious of what is being shared

• Set up a special folder in the root of your Box account called Restricted
  • The Restricted folder must have certain permissions set to disallow the
  • Put all Restricted information in this folder
  • Only provide access to collaborators through a deliberate invitation to each particular user, do not use the option to “Share with a Link”
  • Set up your Box notifications appropriately for the Folder so you are made aware any time your collaborators access your Restricted folder
  • Disable the Sync function for the Restricted folder
  • Encrypt all devices that will be accessing UChicagoBox.

• Enable two factor authentication for your CNET account; accessible at http://2fa.uchicago.edu. This will prevent phishers from accessing your Box account.
Data Guardian Program

The following controls are being established to ensure the proper use of the UChicagoBox system:

1. Scan all BSD UChicagoBox accounts for PHI and PII
   - Check the folder permissions for PHI and PII
     • If the permissions do not meet the required policy, PHI and PII will be moved to a Restricted folder at the root of the user’s Box account
     • A notification will be sent to the user summarizing the activities that took place.

2. Confirm 2 Factor Authentication
   - Check user is enrolled in 2 Factor Authentication
     • If user is not enrolled in 2 Factor Authentication, access to UChicagoBox will be restricted until user enrolls [http://2fa.uchicago.edu](http://2fa.uchicago.edu).

These controls are intended to guide users. To safeguard information users are expected to know and understand associated security requirements and comply with procedures regarding the handling of confidential information.