## RDM WORKFLOW: Secure audio recording in the field

Features:

* Files shared through Box (box.berkeley.edu)
* Files encrypted prior to upload, per IRB/ISP requirement
* Encryption passwords printed and stored in a secure place to avoid data loss
* Encrypted files are reviewed to ensure that they are not damaged.
* After review of encrypted files, files on laptop are deleted for security in the field
* Uses Mac OSX utilities, Box; no additional software required

### WORKFLOW OVERVIEW

**SET-UP**

* ENCRYPTION PASSWORDS: Principal Investigator (PI) creates strong passwords for interviewers, transcripts and herself. In the case that the PI will also conduct and record interviews, the PI should create two passwords, one as interviewer and the other as administrator. (The second password can be used to encrypt the PI’s archive; see below.) PI keeps a paper copy of these passwords securely locked in her office.
* LAPTOP SECURITY: PI creates strong passwords for each interviewer’s laptop, and assigns a password to each interviewer. PI keeps a paper copy of these passwords securely locked in her office. PI must ensure that the laptops meet campus’s requirements for [Minimum Security Standards for Networked Devices](https://security.berkeley.edu/minimum-security-standards-networked-devices-mssnd) (MSSND). Campus Shared Services-IT suggests that the PI have them conduct an IT security seminar at which the interviewers can properly prepare their laptops to meet those requirements.
* BOX: PI creates a Box folder for the project, and creates a project interviews folder and a project transcripts folder within the project folder.

**INTERVIEW RECORDING/FILE HANDLING**

* RECORDING: Interviewers record interviews, place each recording in its own folder on laptop, and encrypt the folder using password assigned by PI.\* Interviewers upload encrypted files to Box. TIP: After transferring each recording to their laptops, interviewers should spot-check the resulting audio file to be sure the transfer was successful prior to deleting the interview from the recording device. The interviewers can check that the file type and the file size are appropriate. Also, they can listen to sections of the audio file to be sure the data has not become corrupted.  
    
  *\* NOTE: This workflow is designed to support use of encrypted disk images by a research team made up exclusively of Mac users. If some team members who will need to access the recordings (e.g., transcriptionists or research analysts) use PCs, encrypted .7z files should be created instead. In that case, third-party software must be used. The recommended tools are: 7Zip (Windows) and Keka (Mac). With these tools, interviewers can encrypt audio files directly; there is no need for them to create an enclosing folder for each recording.*
* QUALITY CONTROL: PI downloads and reviews each file, decrypting the file with the associated interviewer’s password. When satisfied that encryption has not damaged the recording, PI notifies interviewer to delete the unencrypted original recording from the laptop.   
  + *SECURITY NOTE: Project must set (and comply with) a period of time by which   
    each recording will be reviewed and the unencrypted original file deleted from the interviewer’s laptop. One week is an acceptable length of time.*
  + *TIP: The transcriptionist can provide this quality-control check in the course of transcribing the interview.*
* ARCHIVE: PI re-encrypts each file with her admin/archive password and stores it in her archive.

**TRANSCRIPTION**

* Transcriptionist downloads encrypted interview files from Box, and decrypts each with the associated interviewer’s password.
* Transcriptionist transcribes the interviews, removing any identifying elements per plan made with PI.
* The transcriptionist uploads the anonymized transcript files to the project transcript folder on Box. With all identifying elements removed or abstracted, there is no need to encrypt the transcription.
* Transcriptionist deletes both the encrypted interview files and the unencrypted interview recordings from her computer.
* PI reviews transcripts for quality.
* Transcriptionist deletes transcripts on her computer after hearing from PI that the transcriptions are ok.  
  + *SECURITY NOTE: Laptops and workstations used by transcription team must all meet the same MSSND requirements stipulated for interviewers’ devices.*

**RESEARCH & ANALYSIS**

* PI shares project transcript folder on Box with researchers who have approval to access the transcripts.

## RDM WORKFLOW: Secure audio recording in the field

### WORKFLOW DETAILS

**SET-UP**

ENCRYPTION PASSWORDS

* Principal Investigator (PI) creates a strong password for each interviewer to use to encrypt files, including one for herself if she will serve as an interviewer. PI uses Keychain Access on her Mac to create these passwords. If there are too many interviewers to make this process manageable, she can assign shared passwords to groups of 4-5 interviewers. PI compiles a list of these passwords and their associated users, and prints a paper copy that she will keep locked in her office. She then distributes each password to the appropriate interviewer.
* PI securely distributes passwords to transcriptionist. To do so, PI places the list of passwords and associated users in a folder, and, using Mac OS X’s Disk Utility software, encrypts the folder using the transcription password. See <https://support.apple.com/en-us/HT201599> for instructions. PI should make sure that the ‘Save Password in Keychain Access’ checkbox is UNCHECKED in the Disk Utility dialog box. When done, PI provides the resulting .dmg (disk image) file to her transcriptionist. Separately, she communicates the transcription password to the transcriptionist.   
  *NOTE: If the transcriptionist uses a PC rather than a Mac, third-party software should be used to encrypt. See note in overview, above.*
* Transcriptionist decrypts the .dmg file using the transcription password. The disk image will appear on the desktop and a finder window will open displaying the original folder and the file (list of passwords) it contains. The transcriptionist opens the file and prints the list. Then, she ejects the disk image, either by control-clicking the icon on the desktop and selecting ‘Eject’ or by dragging the icon to the trash. Next, she deletes the encrypted .dmg file and empties the trash. The transcriptionist keeps the paper copy locked away securely.
* After the list of passwords is shared with the transcriptionist, PI deletes the encrypted .dmg file and the original folder (with the file it contains) from her computer.
* PI creates an encryption password for herself, separate from the password she will use to encrypt the interviews she records (if applicable). PI will use this second password to encrypt archive copies of the recordings and any other sensitive documents that won’t need to be shared. PI securely stores a paper record of this second password, as above.

LAPTOP SECURITY

* The PI is responsible to ensure that all laptops used to handle sensitive data meet campus requirements established for [Minimum Security Standards for Networked Devices](https://security.berkeley.edu/minimum-security-standards-networked-devices-mssnd) (MSSND). For example, the interviewer’s user account on the laptop must have a strong login password.  
  + *SUGGESTION: Perhaps CSS-IT can provide an IT Security Seminar to explain MSSND requirements and to help interviewers adjust their laptop settings and install required software*
* PI assigns each interviewer an MSSND-compliant laptop or ensures that all laptops used by the interviewers are MSSND-compliant.
* PI may choose to assign MSSND-compliant passwords, in which case she should keep a paper copy of each password and the associated interviewer name or computer ID locked in her office.

BOX

* PI creates a project folder on Box (box.berkeley.edu).   
  + *SUGGESTION: If this project has co-PIs, create a CalNet Special Purpose Account (SPA) and use it to create the project folder. See the* [*CalNet SPA web page*](https://calnetweb.berkeley.edu/calnet-departments/special-purpose-accounts-spa) *for details, or ask RDM for guidance.*
* PI creates a project interview folder within the project folder on Box.
* PI invites each interviewer and the transcriptionist to have [Viewer/Uploader privileges](https://community.box.com/t5/Collaboration-and-Sharing/What-Are-The-Different-Access-Levels-For-Collaborators/ta-p/144) on the project interview folder.
* PI creates a project transcript folder within the project folder on Box.
* PI invites the transcriptionist to have Viewer/Uploader privileges on the project transcript folder.
* PI can also share the project transcription folder with any research team members who have approval to access the transcripts.

**INTERVIEW RECORDING/FILE HANDLING**

RECORDING

* Interviewers create a folder on their laptop for each recording, named per the project’s file-naming convention.
* Interviewers record the interview(s).
* After each interview session, or at the first available break if multiple interviews are held one after another, interviewers transfer each recording from the recording device to the corresponding interview folder on their laptop.
* Interviewers immediately create an encrypted .dmg (disk image) file of the folder using their assigned encryption passwords. (Again, see <https://support.apple.com/en-us/HT201599> for more information.) SUGGESTION: Include the interviewer name as part of the encrypted disk image name to clue PI to which password is necessary to decrypt the folder.
* When internet access is available (strong wifi, at least), interviewers upload encrypted folders to Box by dragging them to the project interviews folder on the Box web site.

QUALITY CONTROL

* PI receives notification (from interviewers, from Box, or from both) that encrypted folders have been uploaded.
* PI downloads each encrypted .dmg file to a folder on her computer, decrypts the file using the associated interviewer password, and, from the finder window that appears, opens the audio file contained within and reviews it for quality.
* Once PI gives the word that the files are ok, the interviewers delete the unencrypted original files from their laptop. At this point, they can also delete the encrypted copies from their laptop.  
  + *SECURITY NOTE: Project must set (and comply with) a period of time by which   
    each recording will be reviewed and the unencrypted original file deleted from the interviewer’s laptop. One week is an acceptable length of time.*

ARCHIVE

* PI drags the folder icon (next to the folder name) of the finder window that opened when she decrypted the .dmg file to a folder on her computer. SUGGESTION: Give the folder to which she drags the folder icon a name such as “Project Interview Archive.”
* Using Disk Utility and her own encryption password, PI creates an encrypted .dmg (disk image) file from the interview folder.
* PI ejects the disk image that has opened on her desktop, either by control-clicking the disk icon and selecting Eject, or by dragging the disk icon to the trash.
* PI deletes the original encrypted .dmg file downloaded from Box, making sure to empty the trash.

**TRANSCRIPTION**

* The transcriptionist receives notification (from Box, from the interviewers and/or from the PI) when an encrypted .dmg file has been uploaded, and downloads the file to her computer.
* Transcriptionist decrypts the file using the appropriate interviewer password, and transcribes the interview, removing any identifying elements per plan made with PI.
* When done, the transcriptionist encrypts the text transcript using the transcript password that the PI has provided and uploads the resulting .dmg file to the project transcript folder on Box.
* Transcriptionist ejects the disk image that has appeared on her desktop and deletes the encrypted .dmg file.
* PI decrypts transcript and reviews for quality.
* Transcriptionist deletes unencrypted transcript on her computer after hearing from PI that the encrypted version is ok.

**RESEARCH & ANALYSIS**

* PI shares the project transcript folder with any research team members who have approval to access the transcripts, and shares the transcript password with them.