Submitting Electronic Records to ORI[1]

The research world has quickly transitioned from primarily hard copy to electronic record keeping. ORI continues to increasingly shift to a digital environment as well. When we receive paper records from institutions, valuable time is diverted to digitizing them. Many RIOs now provide investigation records to ORI in electronic formats, which speeds up our processing time. Because we receive so many questions from RIOs about how electronic records should be submitted to ORI, below are the types of electronic submissions that have been most useful for ORI. As always, contact DIO with any questions at any phase of your case handling.

These approaches have been working well:

- Submit inquiry and investigation reports in electronic format (e.g., a USB drive or external hard drive) via a carrier that provides package tracking information.

  NOTE: If you plan either to encrypt files or to transmit your submission via an online file storage site, first consult with the DIO investigator assigned to the case or the DIO Director to ensure that DIO will be able to access the files.

- If there are multiple respondents, ensure that the report and associated materials clearly differentiate each respondent and relevant materials. Separate reports for each respondent may be needed; consult with the DIO investigator assigned to the case to discuss how to handle these situations.

- All reports include attachments, appendices, or something comparable. When labeling these items, ORI recommends the following:

  ➢ Give the file a brief descriptive name that indicates what is in it. For example, files could be arranged and named like this:

    - *Appendix 1_ transcripts of interviews*
      – *Tab 1.a. Interview of Respondent Dr. Lincoln*
      – *Tab 1.b. Interview of Complainant Dr. Roosevelt*
      – *Tab 1.c. Interview of Witness #1 Dr. Washington*
      – *Tab 1.d. Interview of Witness #2 . . .*

    - *Appendix 2_ grant applications*
      – *Tab 2.a. NCI applications*
        o *Tab 2.a.1. R01 CA . . .*
      – *Tab 2.b. NIAID applications*
        o *Tab 2.b.1. P50 AI . . .*

---

[1] The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

- - *Appendix 3_ published papers and manuscripts*

  - *Appendix 4_ . . .*

  ➢ Do not exceed 140 characters in the names of files; shorter is better!

  ➢ If files are organized in multiple levels of subfolders, do not exceed the maximum limit of 220 characters in folder name and file name combined. Consider compressing the subfolder with content that may exceed maximum limit in combined names to a ZIP file.

  ➢ Do not combine all attachments in a single PDF file, as each attachment must be separate for appropriate electronic filing.)

- For any records submitted separately from an inquiry or investigation report, include a letter with the following information:

  ➢ the sender's name and role at the institution
  ➢ the DIO or ORI number, if one has been assigned by ORI
  ➢ a clear statement about who at ORI requested the materials, if applicable
  ➢ a list of the materials submitted
  ➢ a statement about whether the materials are original records/evidence**

- If the materials submitted are items that were sequestered, provide a chain of custody document or a detailed description of the chain of custody for each item, including the names of all personnel who sequestered the item, made a copy of the item, handled the item, and/or otherwise had custody of the item. Also:

  ➢ for any materials that are electronic copies (e.g., copy of a hard drive), provide a description of the program used to create the copy (see * below for more information)

*Special Requests for Submitting Evidence**

Evidence may consist of hard drive(s), original evidence files in a proprietary format, films, blots, or other materials that DIO investigators may need to analyze directly to develop a report that becomes part of the investigative record.

Hard Drives

- For hard drives (including USB and shared drives), ORI prefers to receive a forensic image of the hard drive in a standard format (e01 or dd). **Do not submit an original hard drive or USB drive without first contacting ORI to discuss the proper handling of these devices**. The following articles from the National Institute of Standards and Technology (NIST) explain how a forensic image can be made:

- ➢ https://www.nist.gov/programs-projects/digital-forensics

- ➢ https://csrc.nist.gov/publications/detail/sp/800-86/final

- ➢ https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

- Chapter 2 of a January 2017 U.S. Attorneys' Bulletin from the Department of Justice provides helpful information on forensic imaging. See: https://www.justice.gov/usao/page/file/931366/download

- For each drive sequestered, provide the following information to the extent possible:

  - ➢ the names of all personnel who sequestered the drive

  - ➢ the names of all personnel who made a forensic image of the drive

  - ➢ the location (building name, room number, and address) and photos of where the drive was located when it was sequestered

  - ➢ a description of the room (e.g., a shared laboratory space or a particular person's office) where the drive was located when it was sequestered

  - ➢ a description of the type of equipment housing the hard drive (e.g., laptop, desktop, or external hard drive), including serial number and property tag number

  - ➢ a complete list of identifying information for the device (e.g., brand, model, and serial numbers) housing the hard drive

  - ➢ a photo of the device in context at the time of sequestration

  - ➢ a complete list and photos of identifying information for the sequestered drive (e.g., brand, model, and serial numbers)

  - ➢ a complete list of identifying information for the forensic image sent to ORI (e.g., brand, model, and serial numbers of the forensic image) and identification of the sequestered drive it represents

  - ➢ identification of the write-blocker used for the forensic image

  - ➢ a complete list of all people who had access to each piece of equipment housing the hard drive

  - ➢ a description of the level of password protected security of the drive, i.e., who had password access to what parts of the drive

➢ a list of general information about the drive, including specific usernames for each person who had access/encryption keys for any encrypted portion of the device that is imaged

➢ log files produced by the imaging software, including verification hash values, preferably MD5

Interviews and Emails

- After each interview, ORI suggests that you provide the witness with the transcript or recording to check whether everything that he/she said was captured correctly and have the witness correct any errors or provide you with written confirmation that the transcript or recording is accurate.

- If figures or other visual evidence are discussed during the interview, please clearly identify vocally – for the transcript -- what is being examined in each case and mark that document with an exhibit number. Please provide a copy of the marked documents to ORI with the transcript/recording.

- If possible, provide ORI a copy of the recording and a written transcript for all interviews; each transcript should be in a PDF format.

- For emails that are not on a sequestered drive, please provide a forensic image of the file(s) or provide PDF copies of the actual emails with all of the attachments. Contact ORI for technical assistance.

Proprietary Formats and Laboratory Materials

- Please consult DIO about potential options.