

Data/Office Security, Research Authorship & FSPH new device training

Dr. Ritz's Research Lab
07/17/2024



Contents

Data & Office Security

- CITI Training
- Data Security
- Office Security

Research Authorship

- Importance
- Authorship Criteria

FSPH new device training



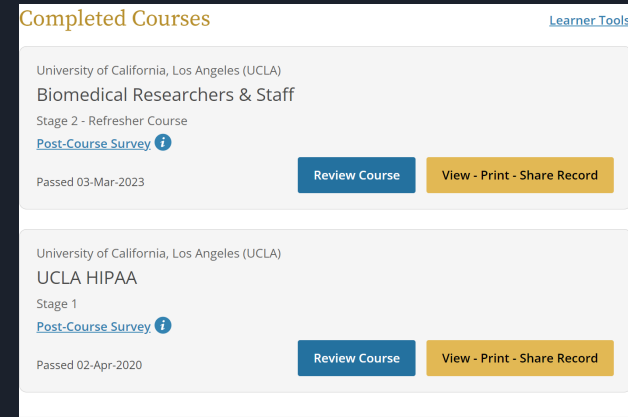
Data & Office Security

CITI Trainings

Everyone within the Ritz Lab is required to take the following two trainings at <https://about.citiprogram.org/en/homepage/> :

- Human Research- Biomedical Researchers & Staff/ Group 1 human subject research (current)
- UCLA HIPAA*

Please keep the certificates updated.



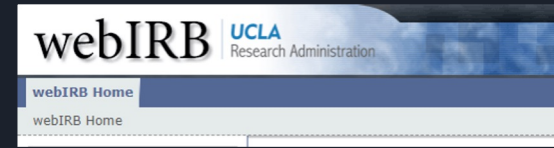
Completed Courses [Learner Tools](#)

University of California, Los Angeles (UCLA) Biomedical Researchers & Staff Stage 2 - Refresher Course Post-Course Survey i Passed 03-Mar-2023	Review Course	View - Print - Share Record
University of California, Los Angeles (UCLA) UCLA HIPAA Stage 1 Post-Course Survey i Passed 02-Apr-2020	Review Course	View - Print - Share Record

*HIPPA: Health Insurance Portability and Accountability Act



Data & Office Security



UCLA webIRB

UCLA's internet-based software application for the submission and review of research projects involving human subjects

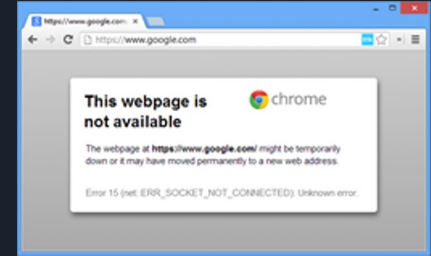
- Each project has an individual IRB approval.

*Both PhD and Master students are required to be included in the relevant IRBs for their own theses/dissertations

*Please ask your advisor for creating an IRB account.

Data & Office Security

Study data of Ritz Lab



There are different types of computers and storage in the Ritz Lab, most cannot be accessed via the Internet.

- **Ritz Server** : (Network attached storage) NAS server connecting most researcher computers via Ethernet (connected to the Internet).
- **PEG-Boss** : PEG study NAS server connecting computers inside the PEG Office (transfer data through switch, not connected to the Internet)
- **Secure computer**: A data enclave that contains personal identifiable data from the state government. (Disconnected from network)
- Encrypted hard-drives and flash-drives: containing de-identified data for sharing with researchers/collaborators
- UCLAHealth BOX (HIPPA compliant limited access – need Mednet email)

*All data sharing within Dr. Ritz's lab should be done via encrypted devices or UCLAHealth BOX.



Data & Office Security

Request and use of data

If you plan to design your own research analysis, you must:

- Submit a signed **Data Request form**.
- The request form and any changes to it must be approved by Dr. Beate Ritz, and/or all collaborating researchers.
- Obtain approval from Drs. Ritz and/or her collaborating researchers before making study data or results available to third parties in any format, including but not limited to:
 - Class assignments and projects
 - Posters/abstracts in conferences
 - Manuscripts submitted to publications
 - ...



Data & Office Security

Research projects datasets

- Return of Data:

Any **programming codes**, **publishable material** (document, tables, figures, etc.), and **secondary datasets** generated from data provided **must be returned** to and/or data manager to be stored in the Ritz network at UCLA

- Code sharing and code checking:

All analyses have to be documented in a manner that anyone from the lab can run and get the same results BEFORE a) publishing, or b) getting a signature from the faculty responsible for a report that contributes to a master's or doctoral thesis and graduation

- Warnings:

A) Data in any form being viewed, handled, or accessed by unauthorized individuals is **not allowed**.

B) **Sharing datasets** with other individuals including **internally** to the research group/UCLA without permission of Dr. Ritz and/or her collaborating researchers is **not allowed**.

Data & Office Security

Data storage - Portable devices

- Password-protected **external hard-drive/flashdrive**.
 - Encrypted by PGP or Bitlocker
- **Do not save** any data or dataset on **unencrypted local personal devices**
- *Regularly backup external hard drives to the Ritz network at UCLA
- Return the external hard drive to the project data manager upon completion of the approved analyses (or expiration of Confidentiality agreement.)
- **Do not include HIPAA identifiers** in any dataset placed on an **external drives**, unless allowed by the IRB and permitted in writing by the PIs.

Data & Office Security

Data storage- Box.com

- UCLA Box vs UCLAHealth Box
 - **UCLA Box** is the personal Box folder linked to student's ucla address for storage of personal data - **NOT HIPAA-Compliant**
 - **UCLAHealth Box - HIPAA-Compliant** data storage, appropriate for storage of study data including personal identifier of study data (must be accessed via **Mednet** account)
- **Do not store** study data on your **personal Box folders** (UCLA or Non-UCLA Box)
 - StudyID including birth year and initials are considered personal identifier.
 - We will create a researcher folder for you on the UCLAHealth Box if needed.
- **Do not store** study data on **other cloud-based storage** (e.g. Dropbox, Google drive)
- While storing data containing HIPAA identifier is allowed on UCLAHealth Box, we strongly recommend to reduce the amount of personal identifier information to minimum.



Data & Office Security

HIPAA personal identifiers

The HIPAA Privacy Rule regulation specifies **18 identifiers**, listed below, most of which are demographic. Inclusion of even one of the following identifiers makes a data set identifiable.

- Name
- *All geographic subdivisions smaller than state, including street address, city county, and zip code, and their equivalent geocodes
- All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- Telephone numbers
- Fax number
- Email address
- Social Security Number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URL
- Internet Protocol (IP) Address
- Biometric identifiers, including finger or voice print
- Photographic image - Full-face photographs and any comparable images.
- Any other characteristic that could uniquely identify the individual

* Exceptions of this identifier could be found at <https://ohrpp.research.ucla.edu/hipaa/>



Data & Office Security

Data containing HIPAA identifiers

- If access to **HIPAA personal identifiers** required, such data should only be worked on project-specific computers in the locked research offices of project's PI at UCLA. **Password protection** must be implemented.
- If access and use off-campus is necessary, researcher must find out if the IRB allows off-campus data use for the respective study.
- Data (digital or printouts) with personal identifiers must never be passed to unauthorized individuals for handling.
- Printouts of with personal information must be **secured in a locked file cabinet**, and **destroyed immediately** when no longer needed.
- HIPAA personal identifiers should NEVER be included in faxes, postal mails, emails, virtual workspaces (e.g. Slack, Zoom, etc.), reports, presentations, publications, etc.
- Any type of publication or presentation listing of individual cases and description of individual cases should be excluded from the researcher.



Data & Office Security

Working on personal devices

- Ensure the personal devices are protected and **not left unattended** at all settings. This includes and is not limited to work, school, home, car or any publicly accessible areas.
- Do not work on your personal device while connecting to **public WiFi**.
- If you are sharing workspaces or devices with other, please make sure to have a separate password protect account for your work.
- If device (laptop, phone, and/or flash drive, etc.) is **lost or stolen**, immediately report this device loss to the office manager, and report relative data loss to data manager. Report to the UCLA Police if necessary (<https://www.police.ucla.edu/prevention-education/education/laptop-theft>).



Data & Office Security

Working on personal devices

*Tips for protection against malicious software on your personal device:

- Keep the operating system and any program you use are up to date with patches/updates.
- Always be wary of any strange emails, especially ones with attachments. Confirm with the sender or IT if needed
- When browsing the internet, always watch out for what you click and install.
- Use a web browser other than Internet Explorer.
- Install anti-spyware/anti-adware if needed:
 - Microsoft Security Essentials
 - Microsoft Windows Defender
 - AVG Internet Security
 - SuperAntiSpyware

*adapted from <https://www.seasnet.ucla.edu/malware/>



Data & Office Security

Office security

- All requests for keys must be made via **Key Request Forms** which can be obtained from the office manager.
- Researchers, staff, and graduate/undergraduate student research assistants are allowed to carry with them **ONLY** the one key that gives access to their main work area.
- Room keys and cabinet keys need to be safely guarded
- Log off/lock the computer workstations if you're done; shut down the computers at the end of the day
- Physical records need to be kept in a secure area
- Always destroy files and documents with confidential data that are no longer needed (e.g., handwritten notes regarding sensitive data)



Additional important notes

1. Doors must be closed and locked before leaving the office
2. Computers must be shut off/log off, folders must be locked in the cabinet
3. Data must be accessed via Mednet account (ongoing)
4. We expect anyone who use the data (PhD/MS/MPH/Posdoc/VS/Staff) should give us a copy for their report
5. Any secondary data generated or coding must be sent back to the lab data manager
6. We encourage co-checkers for analysis, and any people who work on co-checking should be co-author
7. Anybody worked in the lab/paper/coding should always render a summary report (could be R Markdown, MS word/SAS report/Python pandas/Latex)



Research Authorship

Why is it important?

- Authorship confers credit and has important academic, social, and financial implications
- Authorship also implies responsibility and accountability for published work



Research Authorship

Authorship criteria - Who is an author?

- Substantial contributions to the conception or design of the work; or the acquisition, analysis, or interpretation of data for the work; AND
- Drafting the work or revising it critically for important intellectual content; AND
- Final approval of the version to be published; AND
- Agreement to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.



Research Authorship

Authorship & acknowledgement

It's the first author responsibility before any submission, to always ask Dr Ritz or the PI for a specific project about:

- The funding sources that need to be named, including all grants, not only NIH, but also Foundations (ADPA, PD Foundation, etc).
- Who else should be listed as author or included in the acknowledgement



Research Authorship

Non-author contributors

- Contributors who meet fewer than all 4 of the above criteria for authorship should not be listed as authors, but they should be acknowledged.
- Examples:
 - Acquisition of funding
 - General supervision of a research group or
 - General administrative support; and
 - Writing assistance,
 - Technical editing,
 - Language editing,
 - Proofreading
 - ...

Further information please visit: <http://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html>



Additional important notes

- Code check

The analyses (including programming codes, produced tables and figures) must be checked by another person in the lab

- Enhance reproducibility and quality of Lab's research results
- Accelerate learning and collaboration among lab mates
- 1st year PhD or Master students can participate in the code

checking

Anusha M Vable, Scott F Diehl, M Maria Glymour, Code Review as a Simple Trick to Enhance Reproducibility, Accelerate Learning, and Improve the Quality of Your Team's Research, American Journal of Epidemiology, Volume 190, Issue 10, October 2021, Pages 2172–2177, <https://doi.org/10.1093/aje/kwab092>



Practice of Epidemiology

Code Review as a Simple Trick to Enhance Reproducibility, Accelerate Learning, and Improve the Quality of Your Team's Research

Anusha M. Vable*, Scott F. Diehl, and M. Maria Glymour

- Coding errors are common and contribute lack of reproducibility in science
- Even outstanding and highly experienced statistical programmers make mistakes, and much research in health sciences is led by analysts with limited coding experience
- Simple studies can rely on hundreds of lines of code
- Improving the quality of code for data management and analysis should be a high priority for our field

- Code review entails a thorough examination of the data cleaning and analysis methods, including incorporation of explicit tests, by a programmer who was not involved in the initial coding
- Also has secondary benefits: reduces anxiety, increases collaboration, learning, better documentation
- Paper describes specific Instructions for code authors and code reviewers to improve implementation and efficiency of code review
- Also gives examples of code formatting and variable cleaning conventions



FSPH new device training

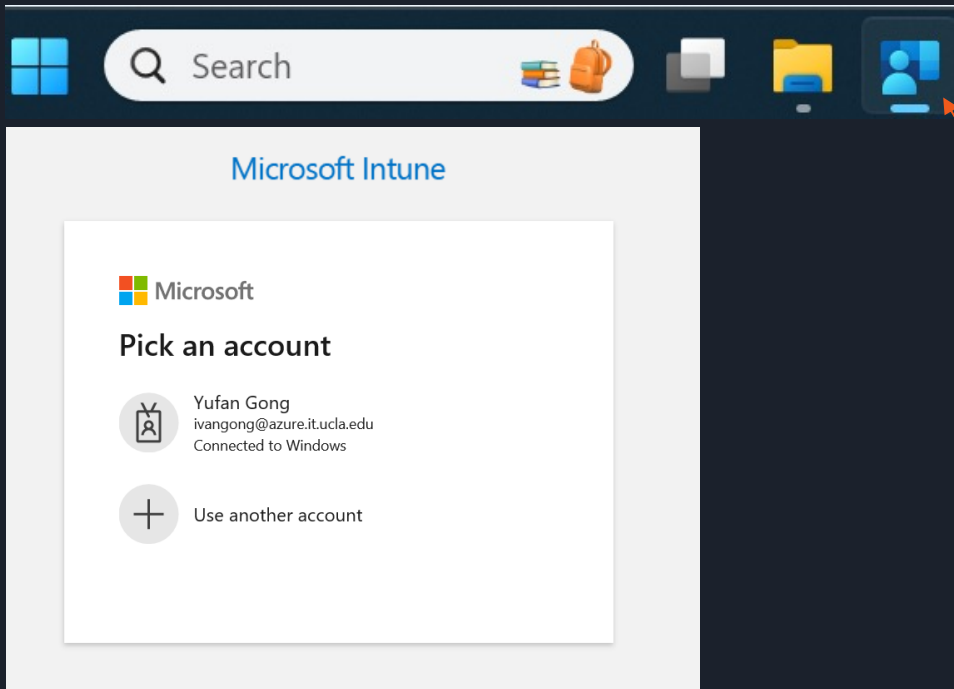
Account and initial password:

- Username: yourUCLALogon@azure.it.ucla.edu
- Password: Welcome2FSPH* (Welcome2ucla*, try this if the first one doesn't work)

Once you logged in, you NEED to change your password!

FSPH new device training

Activate UCLA IT Multi-Factor Authentication (MFA)



Company portal

You will be asked to use the DUO mobile app on your phone to scan a QR code so that you will be enrolled in MFA



FSPH new device training

- **Activate MS Office and Adobe Softwares:**
 - MS office and Adobe Creative Cloud were pre-installed in these devices
 - Adobe (must renew every 120 days): https://ucla.service-now.com/support?id=kb_article&sys_id=c84f45dc1bbbd4d079a486ae6e4bcbf3
 - MS office:
 - Students: https://ucla.service-now.com/support?id=kb_article&sys_id=KB0012869
 - Staff (Mednet): https://uclahsprod.service-now.com/it_portal?id=kb_article_view&sysparm_article=KB0009563



FSPH new device training

- VPN connection (Cisco Secure Client)
 - Campus: ssl.vpn.ucla.edu
 - FSPH: ph.ssl.vpn.ucla.edu
 - Username & password is the same as your UCLA logon



FSPH new device training

- Other pre-installed apps: Google Chrome, Zoom, Slack, BOX drive (can log into UCLA health box)
- You can install other applications to these devices, while some of them require admin privilege. In that happens, please visit: <https://www.it.ucla.edu/> and open a ticket.