DR. BEATE RITZ
DEPARTMENT OF EPIDEMIOLOGY
UCLA, FIELDING SCHOOL OF PUBLIC HEALTH
73-320 CHS BOX 951772
LOS ANGELES, CA 90095-1772
PHONE: (310) 206 7458
FAX: (310) 206 6039

CONFIDENTIAL DATA USER AGREEMENT
OFFICE SECURITY AGREEMENT

Part I. CONFIDENTIAL DATA USER AGREEMENT

In order to ensure the confidentiality of the data collected as part of the research studies conducted by Dr. Beate Ritz and her collaborating researchers, I, _____ will abide by the following listed below.

I will complete the appropriate **UCLA online Collaborative Institutional Training Initiative** (CITI) (e.g. for biomedical and/or for social science research) and the **HIPAA Clinical Research Training Course**, and I will submit a copy of the training certificates to the Office Manager.

PLEASE INITIAL AT THE BEGINNING OF EACH SECTION

____ If I plan to design my own research analysis, I must submit a signed **Data Request form**. The Data Request form and any changes to it must be approved by Dr. Beate Ritz, and/or all collaborating researchers.

____ I will obtain approval from Drs. Ritz and/or her collaborating researchers before making study data or results available to third parties in any format, for example, but not limited to: class assignments, posters or abstracts in conferences, and manuscripts submitted to publications.

____ I understand and will abide to the following requirements about **computers and equipment (including personal devices) used to store and/or analyze project datasets:**

- All computers and equipment (including personal devices) must be password-protected. Such protection will be activated after five minutes of computer inactivity.
- Remote access (if applicable) to project computers located at UCLA via the Internet is prohibited and is prevented by UCLA network security.
- Keep confidential of all the access passwords assigned to me (for computers, files, hard drives, etc).
- Ensure my 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.
- If device (laptop, phone, and/or flash drive, etc.) is lost or stolen, immediately report device) loss to the office manager, and report relative data loss to data manager. Report to the UCLA Police if necessary.
- For further information on security of personal devices and cybersecurity, please visit this website: https://www.it.ucla.edu/taxonomy/term/516

____ I understand and will abide to the following requirements regarding **research projects datasets:**

- Any programming codes, publishable material (document, tables, figures, etc.), and secondary datasets generated from data provided must be shared with PI and/or data manager to be stored in the Ritz network at UCLA.
- I will not allow datasets in any form (i.e. printed or digital) to be viewed, handled or accessed by unauthorized individuals.
- I will keep all datasets confidential at all times and will be held responsible for lapses in confidentiality.
- I am not allowed to share datasets with other individuals including internally to the research group/UCLA, except under express request from Dr. Ritz and/or her collaborating researchers, or a designed person from the team.

____ Project datasets used outside the research project offices, will be shared via **UCLA Health Sciences Box (Mednet Box, not the general UCLA Box)** or in a password-protected **external hard drive.** I understand and will abide to the following requirements when working with research projects datasets:

- Researcher's assigned external hard drive and the sub-folders on Mednet Box are the only locations where project datasets may be stored when outside of the research offices. At no time shall researcher save any data or dataset on local personal devices or any cloud-based storage.
- Researcher is required to regularly back up the external hard drive to the Ritz network at UCLA under Researcher's secure folder or on Mednet Box. The external hard drive is to be backed up at least once a month, or when researcher has added significant amounts of contents including programming codes, secondary data, etc..
- Researcher is required to return the external hard drive to the project data manager upon completion of the approved analyses or expiration of this Confidentiality agreement, whichever occurs first.
- At no time will HIPAA identifiers be included in any dataset placed on an external hard drive and Box.com, unless allowed by the IRB and permitted in writing by the PIs, according to the conditions listed next.

____ If researcher requires access to **HIPAA personal identifiers** (i.e. names, addresses, phone numbers, birth dates, Social Security numbers, geocodes, etc.) the following conditions must be met:

- Researcher will work with such data only on project-specific computers in the locked research offices of the respective project's Principal Investigator at UCLA. Researcher must implement password protection as above.
- If access and use off-campus is necessary, researcher must find out if the IRB allows off-campus data use for the respective study. If it is, _____, the Principal Investigator (PI), must approve this use before the data manager can distribute the necessary datasets. This approval will be noted on a separate document provided by the data manager.
- If researcher requires printouts of personal information, such printouts must be secured in a locked file cabinet whenever researcher leaves the research office. Such printouts must be destroyed immediately when no longer needed. Printed data with personal identifiers must never be passed to unauthorized individuals for handling.
- At no time will HIPAA personal identifiers be included by researchers in postal mails, emails, virtual workspaces (e.g. Slack, Zoom), faxes, reports, presentations, publications, etc.
- If subject/control ID numbers must be e-mailed, they can only be e-mailed independent of any other data or datasets.
- I agree to exclude from any type of publication or presentation listing of individual cases and description of individual cases.

____ Before I terminate my work with _____ (PI), computer accounts (user ID and password) and access to Box will be terminated, and all office-related equipment's and devices will be returned to the data/office manager on or before the date of termination.

____ I have read the above and agree to be bound by the provisions thereof. I understand my responsibility to preserve confidentiality includes the active support of these procedures at all times and that accidental breaches will not be excused. If I notice any violation or potential violation of the terms of this Agreement, I will immediately report it to the Principal Investigator.

_____
Printed/Typed Name

_____
Signature Date

_____ _____
Job Title/Formal Affiliation with Research Study/Project under Dr. Beate Ritz

_____ _____
Telephone Numbers E-mail Address

Part II. OFFICE SECURITY AGREEMENT

Office Keys

All requests for keys must be made via **Key Request Forms** which can be obtained from the Lab Manager. This Key Request Form should be completed and submitted to either Cristina Ruiz or to Dr. Ritz. No one else on the Ritz team is an authorized co-signer for Key Requests.

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. Keys for the other offices in which they may need to work or look for files etc. should be stored securely in their main work area. No one should be carrying around more than one key. This is meant to increase security of our data and the protected health information of our participants and to minimize damage should keys be lost or stolen.

When keys are misplaced/lost/stolen, the corresponding doors, particularly the outer doors, must be re-keyed (several hundred dollars per door). Things happen, to all of us, but if you lose your keys, and more than one key is lost, you may be held financially for re-keying the pertinent doors.

Office Security

- **ALWAYS destroy files and documents with confidential data that is no longer needed**. Confidential information includes but not limited to: HIPPA Identifiers/Personal Identifiers(PID) such as names, addresses, phone numbers, birth dates, Social Security numbers, geocodes, etc.
    1. This applies to interviewers jotting down information about new recruited individuals who wish to enroll, but this can apply to many other things, such as old patient files.
    2. For any project documents, instruments, etc., be sure they have been scanned and saved in a secure area.
    3. Never download or store PID locally on your workstation from the server.

- **NEVER e-mail confidential data and/or personal identifiers**. Particularly to researchers. Researchers are prohibited from seeing personal identifiers such as name, SSN, address, and other contact information.
    1. If identifying subjects, refer to their study subject ID. If new recruited individuals call in wishing to enroll, write their information down on a piece of paper and place it in a locked cabinet. To notify others in the office of the recruited individuals, email them the whereabouts of the paper rather than emailing the confidential information.
    2. When requesting data, it is important to provide the data distributor (Kimberly Paul or Keren Zhang) an encrypted device to obtain the data. To obtain an encrypted flash drive, notify Keren.
    3. De-identified data can be sent over the internet (i.e. email, **Box**), but password protection is recommended. PGP encryption and Microsoft Tool's password encryption feature are both FIPS 140-2 compliant and therefore IRB approved. WinRAR file compression's password protection is not FIPS-compliant but will suffice in sending de-identified data.

- **ALWAYS make sure that all physical records are kept in a secure area at all times**. Switch users or log off your computer (unless someone has told you to allow them to use the computer immediately after you've finished).
    1. All locked cabinets contain important items from patient files to expensive hardware -- lock the cabinets that are open when unattended.
    2. The office must be occupied at all times by at least one person for the office door and cabinets to be unlocked. If you are the last person in the office, please lock the door and cabinets or wait until another person returns before you leave.
    3. Make sure any physical confidential information records are NOT laying around on your desk but are in a locked cabinet or drawer when unattended. This includes:
        a. Faxes with confidential information are not left unattended, and fax machines are in secure areas.

b. Mailings with confidential information are sealed and secured from inappropriate viewing; mailings of 500 or more individually identifiable records of PID in a single package, and all mailings of PID to vendors/contractors/co-researchers are sent using a tracked mailing method, which includes verification of delivery and receipt, such as UPS, U.S. Express Mail, or Federal Express, or by bonded courier.

c. Confidential information in paper form must be disposed of through confidential means, such as crosscut shredding or pulverizing.

d. All disks with confidential information must be destroyed.

4. Confidential information in paper or electronic form, e.g., stored on laptop computers and portable electronic storage media (e.g., flash drives, hard drives, CDs), must never be left unattended in cars or other unsecured, publicly accessible locations.

- **NEVER leave an office door unlocked if confidential data is out in the open and vulnerable to theft or exposure to unauthorized individuals**. It's also good practice to leave the door locked if it's not occupied with our team members, because there's been a rash of theft in this building.
- **ALWAYS make sure that our cabinet keys and room keys are always safely guarded**. Losing keys means creating new vulnerabilities for our data.

1. Record that you have checked out a key and that you have returned it to help us keep track of where it was last used if an investigation is needed.

Furthermore, if you are the last person in the office for the day, please take note of the above as well as the following:

2. **Turn off** the lights and lock the door.
3. **Shut down** all computers (and their monitors) you were working on (refrain from just logging off). Make sure the computer is shut off completely before leaving, as it is possible for the computer to stop shutting down when a command window pops up. Shutting down the computers will help us save power on campus as well as ensure the security and safety of our computers and data.
4. Please also make sure the desk you were using is **clean and organized** (not cluttered with pens, papers, other stationaries, etc.). Throw away any trash that needs to be thrown out, including the cups you have been using for drinking water! A clean office is a happy office -- a messy office is very difficult to work with! The next person working on your desk after you leave for the day will greatly appreciate it!

- Before termination of work with _____ (PI), computer accounts (user ID and password) and access to Box will be terminated, and all office-related keys, equipment's and devices will be returned to the data/office manager on or before the date of termination.

I have read the above and agree to be bound by the Ritz team's **OFFICE SECURITY POLICIES OF SEP 23, 2020**.

Name (please print): _____

Signature: _____

Date: _____

Please return these agreements to the Lab Manager, once you have read the policy and printed/signed your name above.