Scientific Quality Reviewer Guidelines

The CTSA Consortium SRC Pilot Study will conduct *scientific quality reviews* on randomly selected protocols from the baseline and intervention phases of the study. These reviews will be conducted using guidelines similar to those for NIH peer reviews to ensure confidentiality, security, and no conflict of interest (COI). The Scientific Quality Reviewer guidelines, modeled after NIH peer review policies and practices, are outlined below.[1]

Conflict of Interest

As a Scientific Quality Reviewer, you must:

- Screen the protocols assigned to you to determine, to the best of your ability using the available protocol information, if there is real or apparent COI for yourself. Definitions for real or apparent COI can be found at http://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-069.html.

- Immediately inform the Tufts CTSI Project Manager if you are assigned to a protocol with which you have a COI.

  Liza Patchen
  Project Manager, Tufts CTSI
  epatchen@tuftsmedicalcenter.org
  617-636-5751

- Sign the pre-review Conflict of Interest Form certifying that you will identify, to the best of your ability using the available protocol information, any protocol with which you have a COI or appearance of COI.

You **may not** conduct the scientific quality review of a protocol if you can determine from the available protocol information that there is COI:

- You are named in a major professional role on the protocol assigned to you for review.
- The PI or others with a major role in the study are affiliated with an organization to which you also are affiliated.
- Within the past three years, you have been a collaborator or have had any other professional relationship (e.g., served as a mentor) with any person on the protocol with a major role.
- The funding application that supports the protocol includes a letter of support or reference letter from you.
- You have served as a member of the advisory board for the protocol under review.

Confidentiality/Non-disclosure

It is critical that the Scientific Quality Reviewers ensure the protocols they are assigned to review remain confidential. Below are confidentiality and nondisclosure rules for participating Scientific Quality Reviewers to follow.

[1] The Scientific Quality Reviewer guidelines outlined in this document borrow from the NIH peer review policies and practices found at https://grants.nih.gov/policy/peer/index.htm. The Tufts CTSI SRC Pilot Study Team is fully responsible for the content of this document.

Rules related to the confidentiality of information disclosed to Scientific Quality Reviewers in the course of the CTSA Consortium SRC Pilot Study scientific quality review ***prohibit*** a Scientific Quality Reviewer serving on a review from performing certain actions:

- Sharing protocols or review materials with anyone outside the Tufts CTSI project team for the CTSA Consortium SRC Pilot Study
- Granting anyone access to any secure computer system using his or her password or credentials, or through shared communication
- Disclosing, in any manner, information about the scientific quality review deliberations, discussions, evaluations, or documents to anyone outside the Tufts CTSI project team for the CTSA Consortium SRC Pilot Study
- Disclosing, in any manner, information about the review related to a protocol to anyone outside the Tufts CTSI project team for the CTSA Consortium SRC Pilot Study
- Using information contained in an assigned protocol for his/her personal benefit or making such information available for the personal benefit of any other individual or organization
- Disclosing procurement information prior to the award of a contract
- Participating in scientific quality review without signing a confidentiality certification.

The Tufts CTSI project team for the CTSA Consortium SRC Pilot may take steps in response to a violation of the above rules, in order to preserve the integrity of the scientific quality review process. Depending upon the circumstances, such steps may include but are not limited to:

- Notifying or requesting information from a Scientific Quality Reviewer
- Terminating a Scientific Quality Reviewer's service.

Security

Participating Scientific Quality Reviewers are expected to abide by the following security guidelines.

Electronic Security

1. **The single most important advice:** Download the assigned protocols and related materials to a secure PC under your control; do not use unsecured wireless, network drives or servers (i.e., computers and Wi-Fi in business centers or hotels). If using a home-based wireless connection, consider using Wi-Fi Protected Access 2 (WPA2) instead of WEP (Wired Equivalent Privacy—which can be hacked in minutes). Consider downloading materials to a directory so documents can be easily purged after the review.

2. Never post the assigned protocols and related materials on any website or save them "in the cloud" because the files can be "discovered" by internet search engines, e.g., Google or Bing. Make sure you do not disclose any sensitive protocol-related information via social media

websites or to anyone not on the Tufts CTSI project team for the CTSA Consortium SRC Pilot Study.

3. Have a strong password for computer access and never share it. Because professional hackers have software programs that can correctly guess most passwords in less than 10 minutes, please ensure that your passwords are complex and have at least eight characters.

4. If you leave your office, close the protocol file, or lock your computer.
    - Windows-based systems can be locked by hitting the Ctrl, Alt and Delete keys simultaneously and selecting "Lock Computer" from the Task Manager.
    - Consider installing a password-enabled screen saver that activates after 15 minutes of inactivity.
    - Systems can be put into a *sleep* mode and should require a password to wake up.

5. Refrain from sending sensitive protocol-related information in email (even to yourself); it's not secure and could be intercepted. If you must send information related to a protocol you may send the information to the Tufts CTSI Project Manager through email, but only if it is encrypted and password protected and if the Tufts CTSI Project Manager knows how to remove the password protection. Before sending the information, carefully review the message content, eliminate any unneeded confidential information, and then double check the accuracy of the recipients before hitting the send button. If this secure email process is not available for you, please notify the Tufts CTSI Project Manager and an alternative secure process will be identified.

6. Most operating systems can run an encrypted file system to protect files while they are on your hard drive (e.g., Windows - BitLocker and Mac - File Vault 2 and/or encrypted disk images). Consider applying such encryption on your PC. All laptops, however, **must** be encrypted due to the risk of their being stolen or misplaced.

7. All mobile devices (including Blackberries, iPhones and iPads) and portable media (including flash drives, CDs, DVDs etc.) containing protocols and any other protocol-related sensitive materials) **must** be encrypted. Please be aware that handling, storing, or accessing sensitive information on a mobile device is not recommended.

8. Full disk encryption is highly recommended, especially for laptops.

Physical Security

1. If the protocols and/or related materials are in hard copy or reside on mobile devices or portable media (e.g., CD, Smart Phones, flash drive or laptop), *treat them as though they were cash*.
    - Do not leave them unattended or in an unlocked room.
    - Consider locking them in a locked cabinet or drawer.
    - Keep confidential information out of sight when visitors or family members are present.
    - Take extra precautions with mobile devices and portable media. Mobile devices are more susceptible to lost and theft, anti-virus software is not as effective for them; they can store as much or more data than a PC, and can access networks faster.
    - Be particularly careful with flash drives which are small and easily misplaced.
    - Monitor your laptop as it passes through TSA security at the airport and promptly pick it up. Never place it in checked baggage.

2. When the scientific quality review is over, destroy all review-related materials.
   a. Shred hard copies – preferably using a cross-cut shredder.
   b. Delete electronic files securely:
      - At minimum, delete the files and then empty your recycle bin.
      - Optimally, use a ***secure*** **erasure** method, e.g., an electronic "shredder" program that performs a permanent delete and overwrite.
      - CDs can be broken, crushed, incinerated, shredded, or melted.

IMMEDIATELY REPORT lost, stolen, or inappropriate disclosure of a CD, laptop or other data-storage device that contains sensitive data or protocol material. Report to Tufts CTSI Project Manager within 24 hours:

- The scientific quality review protocols in which you are or were a reviewer
- All materials that are missing and whether they were encrypted
- Circumstances surrounding their disappearance (stolen from your office, left in a taxi, etc.).