Appendix 9. Policy on Privacy and Confidentiality of Information Managed by the Coordinating Center

1. Mission of the Collaborative Studies Coordinating Center

The Collaborative Studies Coordinating Center (CSCC) is a division within the Department of Biostatistics of the School of Public Health at the University of North Carolina. As the coordinating center for a number of multi-center public health and medical studies, it provides statistical and scientific direction, data management, quality assurance, and study management expertise and services. The Coordinating Center's typical responsibilities for clinical trials and epidemiological studies include:

- develop and implement plans for acquisition, transfer and management of data about volunteer participants in the studies;
- develop and implement study participant tracking systems;
- organize, analyze and report quality control data for the measurements and interventions;
- perform data analyses;
- provide reports and analyses to study monitoring boards
- collaborate in the preparation of scientific publications and presentations;
- serve as a repository for study materials and data;
- archive study data and related information and produce public use versions of the data,
- facilitate financial, contractual, and accounting matters as the central coordinating center for studies involving multiple clinical sites, data safety monitoring boards, and multi-institutional collaborations.

In providing these functions, the CSCC is subject to a variety of requirements for protecting the confidentiality and privacy of the information. This policy outlines the responsibilities of all CSCC employees (faculty, staff, and students).

2. Introduction – Types of Research Information Managed at the CSCC

Most information handled at the CSCC describes individuals (usually a participant in one of the public health studies coordinated by the CSCC). As detailed below, every CSCC employee has ethical and legal obligations to appropriately protect the privacy of participant information.

In addition to protecting privacy of participant data, many of the research results (statistical analyses, reports and manuscripts), produced by CSCC, must be handled confidentially.

Many of the studies performed at the CSCC are "masked" or "blinded". This means that no one outside the CSCC is allowed to see any results (statistical analyses, tabulations, graphs, etc.) during data collection. The Principal Investigator or Project Manager for the studies on which you work can provide specific information on requirements for your work.

All of our studies result in the development of manuscripts for publication in the scientific literature, presentation at professional conferences, etc. These manuscripts are usually the proprietary (copyrighted) intellectual property of the authors. These authors are typically faculty and staff both here and at the various institutions we collaborate with in the studies (clinical centers, laboratories, etc.). As such, publication or sharing of this material may not be permissible until the information is in the public domain.

Additionally, some of our studies are performed under contracts with private industry (chiefly pharmaceutical companies). These contracts typically include requirements for confidentiality concerning data, analyses, and manuscripts.

3. Policy Statement

It is CSCC policy that, as a condition of employment, all employees shall handle information managed by the CSCC in accordance with this policy and in compliance with all relevant University policies for electronic media and for information management. **A violation of this policy may result in disciplinary action, up to and including dismissal from employment, as provided by University policy.**

4. Definitions

4.1 Privacy: the right of individuals, groups, or institutions to determine for themselves when, how, and to what extent identifiable information within the possession of CSCC is communicated to others.

4.2 Confidentiality: the protection of individually identifiable data, and/or analyses and tabulations of data from research in progress, from use by unauthorized persons and/or for unauthorized purposes.

4.3 Security: The protection of data from accidental or intentional, and unauthorized modification, destruction, or disclosure.

4.4 Individually Identifiable Data (IID): Information which is linked to personal identifiers (see below). IID includes but is not limited to source documents (medical records, data collection forms, death certificates, etc.) and transcribed versions of that information (data files, data listings, etc.). Both hard-copy (paper) and electronic formats are included.

4.5 Personal Identifiers: characteristics (data values) which, separately or in combination, can be used to associate information with a specific individual. Typical personal identifiers include: name, social security number, medical record number, telephone number, birth date, gender, address, ethnicity, etc. However, there are other data elements that may be indirect identifiers that facilitate deductive disclosure of an identity because of the relative rarity of particular combinations of the variables (e.g., a 30-year old woman with a Myocardial Infarction).

The Health Insurance Portability and Accountability Act (HIPAA) is the major federal regulation now defining privacy standards for medical data. HIPAA defines identifiers as any of the following data elements if they are disclosed from the records of a health care provider, health plan or health care clearinghouse:

- Names
- Geographic subdivisions smaller than a state
- Zip codes
- All elements of dates except year directly related to an individual, including birth or death or dates of health care services or health care claims
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security Numbers
- Medical records numbers
- Health plan beneficiary identifiers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URL)
- Internet protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images
- Any other number, characteristic or code that could be used by the researcher to identify the individual

Although CSCC activities are generally *not* subject to the HIPAA regulations, they are becoming a de-facto standard for handling health information in many settings. In particular, NIH is using the HIPAA standards as a model in developing policies for handling of data in NIH-sponsored studies.

4.6 Miscellaneous Protections: Further, particular studies being conducted at the CSCC will often have additional categories of information that must be treated confidentially - for example, occurrence of clinical endpoints such as myocardial infarction, genetic information, use of illicit substances or drugs, or hospitalizations.

4.7 Masked Analyses: Listings, tabulations, graphs, statistical computations, etc. which provide information about the unpublished results of a study. The precise determination of which results should be masked is study-specific and made by the Principal Investigator (PI) and / or Project Manager (PM) of the study. *In general*, data collected prior to the start of a participant's treatment (e.g., medical history, baseline physical exam) and data concerning study quality (e.g., percentage of missing data

forms) are not masked. All data concerning the effect of treatment (side effects, efficacy, etc.) are virtually always masked.

4.8 Format and content of confidential material: The CSCC defines confidential material as any of the following:

a. Any hard copy or electronic file that contains "blinded" (masked) information. (The project manager for each project maintains a list of staff approved assess to blinded information.)
b. Any hard copy or electronic file that contains personal identifiers or individually identifiable data as defined in 4.5 above.
c. Paper or electronic files of unpublished manuscripts and proposals.
d. Paper or electronic files of proprietary information for which there are confidentiality obligations pursuant to an agreement with the proprietor.

5. Protection of participant rights, privacy and confidentiality

5.1. Ethical considerations

In exchange for the cooperation provided by study participants (often without any direct benefit to them), the CSCC represents it will promise to treat confidentially information they provide. The CSCC also represents that use of the information will be limited to the purposes stated when they agree to participate through informed consent; when they agree to provide access to their protected health information through an authorization; or when the IRB approves a waiver of these documents based on protection of the individuals in the design and conduct of the research.

5.2. Practical considerations

Participants in our research projects are often asked to provide information that they would not want publicly disseminated. Their confidence that the information will not be released will have an effect on their willingness to participate and on the accuracy of the information they provide.

5.3. Legal considerations

Several Federal and State laws impose requirements on researchers regarding privacy, confidentiality, and security. Relevant laws and corresponding regulations include:

Privacy Act (PL-93-579, 1974)
National Research Act (PL-93-348, 1974)
Health Insurance Portability and Accountability Act (HIPAA) (45 CFR 160 and 164)
Relevant Federal regulations on medical research
    45 CFR 46, 21 CFR 50 and 56: Protection of human subjects
    FIPS 41: Computer security guidelines for implementing the privacy act
Relevant state laws
    State Privacy Act, State of North Carolina – medical privacy (Chapter 126)
    State Personnel Act, State of North Carolina

Additionally, contracts impose confidentiality requirements. Informed consent and authorization documents are one form of contract with research subjects that may include

confidentiality and privacy obligations. Research sponsorship agreements and various other contracts and grants may also contact confidentiality provisions.

There are also other University information privacy and security policies, including:

The University of North Carolina at Chapel Hill Privacy of Protected Health Information Policy;

The University of North Carolina at Chapel Hill Information Security Policy.

6. Motivations for masking analyses

Results of analyses of data collected early in a study (interim analyses) often differ from the eventual results of the complete dataset. With small amounts of data, the influence of random chance is relatively greater. Clinical center staff may still be learning to conduct certain aspects of the study. Participants recruited early (and from clinics starting recruitment early) may differ from those recruited later. For reasons such as these, the results of interim analyses are often over-interpreted. This over-interpretation can have a variety of undesirable influences on the following aspects of the research:

1. Lowered enthusiasm for recruiting patients and conducting the study
2. Tainted selection of eligible patients
3. Use of concomitant therapies
4. Willingness to discontinue therapy in the face of side effects
5. Bias in subsequent data collection and interpretation

7. Implementation

All handling of confidential data must be in accord with University policies, applicable laws, and the terms and conditions of relevant contracts and consents. The following specific practices are required under this policy for all confidential data:

7.1. Handling individually identifiable data

1. The Project Manager for each project will maintain a written list of persons approved to access IID. The list will be reviewed and initialed by the project PI.
2. Hard-copy of IID will be stored in locked space (e.g., drawers in a locked filing cabinet, a locked room within the CSCC), accessible only to approved staff. When in use, hard-copy IID may be temporarily and securely stored in any reasonable location within the CSCC office space, as needed.
3. Electronic copies of IID will be stored in subdirectories on network volumes, accessible only to approved staff (e.g., restricted directories, password- protected files). When in use, electronic copies of IID may be temporarily stored on local storage devices and / or removable media located and stored within the CSCC office space, as needed. Electronic and hard-copy IID are to be used only to meet specified project objectives.
4. Electronic or hard-copy IID will not be distributed or used outside the CSCC without prior review and approval by the appropriate project PI or PM.

7.2. Handling masked analyses

1. The Project manager for each project will maintain a written list of staff approved to perform and / or access masked analyses. The list will be reviewed and initialed by the project PI.
2. Data files containing treatment assignment information will be stored in subdirectories on network volumes, accessible only to approved staff (e.g., restricted directories, password- protected files). When in use, electronic files with treatment assignment information may be temporarily stored on local storage devices and / or removable media located and stored within the CSCC office space, as needed.
3. Data files containing treatment assignment information will be used only to meet specified project objectives, as authorized by the Principal Investigator. Files should be used only by individuals with permission to perform analyses authorized for project.
4. Hard-copy of masked analyses will be stored in locked space (e.g., drawers in a locked filing cabinet, a locked room within the CSCC), accessible only to approved staff. When in use, hard-copy masked analyses may be temporarily and securely stored in any reasonable location within the CSCC office space, as needed.
5. Electronic copies of masked analyses will be stored in subdirectories on network volumes, accessible only to approved staff (e.g., restricted directories, password- protected files). When in use, electronic copies of masked analyses may be temporarily stored on local storage devices and / or removable media located and stored within the CSCC office space, as needed.
6. Electronic or hard-copy masked analyses will not be distributed or used outside the CSCC without prior review and approval by the appropriate project PI or PM.
7. Masked analyses should be discussed only with CSCC staff authorized to access masked analyses. In particular, it is rarely appropriate to discuss masked analyses with clinical center investigators or clinic staff. Access of other individuals (such as Project Office staff, members of external boards or committees, etc) is study specific (and sometimes situation specific) and must be approved by the appropriate CSCC PI or PM. Masked analyses should never be discussed with reporters or individuals not specifically related to the project.

7.3. Applicability, exceptions

All questions concerning the application of these procedures to a particular data case of data access, reporting, or analysis should be referred to the PM or PI. Conflicts or disagreements that can not be resolved at that level should be referred to the CSCC Director for review and resolution.

8. Disposing of confidential material

1. What is Confidential

   For the purpose of disposal, the CSCC defines confidential material as described in Section 4.8.

2. What to put into the Confidential Trash System

   Only those pages of paper/printout that meet the definition of "CONFIDENTIAL" are to be placed in the confidential trash system.
   For example, if a printout contained 200 pages and only 3 pages of the printout are confidential, then only the 3 pages should be placed in the confidential trash. The remaining pages should be recycled.

3. Accumulation and Pick Up of Confidential Trash

   Under the confidential trash system
   a. Each employee who handles and/or maintains confidential information will accumulate and sort CSCC-designated confidential trash in his/her office. The employee will remove all paper clips, rubber bands, etc. from the paper.
   b. When the employee has sufficient confidential trash, he or she will request a confidential trash pick up through "Assist" (the CSCC Network Support Group).
   c. A member of the Assist staff will come to all the offices that have requested a pick up and take properly sorted confidential trash to the storage area in the secure forms room.
   d. Assist will contact the University contractors who will pick up the confidential trash and shred it.

4. Disposition of Confidential Electronic Files

   All electronic media must be properly sanitized before being transferred from the custody of its current owner. The proper sanitization process depends on the type of media and the intended disposition of the media.

   Any employee who stores confidential information in electronic format on removable media such as floppy disks, Zip drives, CDs or memory keys, is responsible for removing the information or destroying the medium if erasure is not possible.

   When computers are reassigned to new employees, transferred to other departments or sent to surplus, Assist will remove all information from the hard drive by using a data removal utility. Equipment designated for surplus or

other disposal will have a label affixed stating that the hard drive has been properly sanitized.

5. Reporting Lost or Stolen Confidential Electronic Files

   If electronic media (either removable, or internal to a system) are lost or stolen, and/or if confidential data is disclosed, the CSCC employee with knowledge of this matter should report to the Project Manager or the Project Principal Investigator who will determine additional action required.

9. Personnel and Financial Information

9.1. Personnel Information. Certain CSCC staff handle and/or maintain personnel information that may be confidential under State law. Confidential personnel information includes employment applications, performance reviews, disciplinary actions, and personal and financial information (More information is available on the University Human Resources website http://hr.unc.edu). All CSCC employees are expected to observe confidentiality during activities such as recruitment, performance reviews, or disciplinary actions for which they are responsible. CSCC employees are expected to observe confidentiality in all situations in which access occurs for personnel information that would not normally be available or under their direct supervision; for example, access occurs from shared printers, internal mailboxes, copier and FAX use, shared conference rooms.

9.2 Financial Information. Principal Investigators and their designees and CSCC Administration are authorized to have access to grant and contract budget information for active projects and proposals under development. Financial information should be shared only for essential business purposes, and all CSCC employees are expected to maintain confidentiality when accessing sensitive financial information. Financial information for the CSCC is generally accessed by administrative personnel through various password-protected electronic systems. Financial reports are maintained in locked file cabinets under the supervision of the Administration Division of the CSCC. Research team members who are provided financial information for business purposes are responsible for maintaining confidentiality in handling these matters.

10. Rules of Behavior for Information Technology

In addition to the policies described above, employees are also required to abide by the CSCC Rules of Behavior for Information Technology. These Rules of Behavior are specified in a separate document.

Policy on Privacy and Confidentiality of Information Managed by the CSCC

Acknowledgement and Agreement

NAME OF EMPLOYEE_____

DATE OF MANDATORY GROUP TRAINING _____

(The employee is required to sign this form as a condition of employment.)

1. The following individuals have reviewed this document with me. I understand and accept these requirements of employment.

_____ _____
Employee's Signature Date

2. I reviewed this policy with the employee signing above and believe that (s)he understands and accepts these job requirements.

_____ _____
CSCC Confidentiality Policy Committee Representative's Signature Date

[Following reviews and signatures, return only this original page to the CSCC Administrative Office for insertion (inclusion) in the employee's personnel file. Copies may be retained by supervisor and employee.]

Collaborative Studies Coordinating Center

Rules of Behavior for Information Technology

Introduction

These CSCC Rules of Behavior for Information Technology are based on NIH Information Technology General Rules of Behavior which, in turn, summarized laws and guidelines from various NIH and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002.

What are Rules of Behavior?

Rules of Behavior are part of a comprehensive program to provide fully integrated information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

Who is Covered by These Rules?

These rules extend to all CSCC personnel and any other persons using or accessing CSCC information technology (IT) equipment, resources or data. All users should be fully aware of, and abide by, CSCC security policies

What are the penalties for Non-compliance?

Users who do not comply with the prescribed Rules of Behavior, are subject to penalties that can be imposed under existing policy and regulations, including official, written reprimands, suspension of system privileges, temporary suspension from duty, removal from current position, termination of employment, and even criminal prosecution. CSCC will enforce the use of penalties against any user who willfully violates any CSCC system security (and related) policy as appropriate.

The CSCC Rules of Behavior are founded on the principles described in the NIH published security policies and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget regulations and Standard of Conduct for Federal Employees. Therefore, these Rules of Behavior carry the same responsibility for compliance as the official documents cited above.

Accountability-General Requirements

Users:

- Users should behave in an ethical, proficient, informed, and trustworthy manner.
- Users shall not attempt to override technical or management controls.
- Users should complete the CSCC Confidentiality Training and the on-line Collaborative Institutional Training Initiative (CITI) Training prior to obtaining access to work on an NIH contract.
- Users must employ up-to-date virus protection software.
- Users should use only systems, software, and data for which they have authorization and use them only for official business.
- Users must report security incidents, or any incidents of suspected fraud, waste or misuse of CSCC systems to the project manager or Principal Investigator of the study

concerned. If the incident is not specific to a particular study it should be reported to the CSCC IT Manager, Director or Deputy Director.
- Users must protect confidential and/or sensitive information from disclosure.
- Users shall not store sensitive information on portable devices such as laptops, PDAs and USB drives or on remote/home systems unless they have written authorization from the study Principal Investigator and encryption is employed. For non-study data the written authorization must be provided by the CSCC Director or Deputy Director.
- Users must protect passwords from access by other individuals.
- Users should change passwords frequently, no less often than every six months.
- Users must protect university and government property from theft, destruction, or misuse.
- Users shall not remove computers from CSCC premises unless authorized in accordance with CSCC property management requirements.
- It is the responsibility of users to ask IT staff for assistance if they do not know how to comply with procedures, such as encrypting information on USB drives, setting computers to download and install critical patches automatically, etc.

Managers:

- Ensure that staff are given access to, and ample time to complete, the CSCC Confidentiality Training.
- Ensure that staff are provided access to, and are aware of, all existing CSCC policies and procedures relevant to the use of CSCC information technology resources and the protection of sensitive information.
- Require that staff follow system security policies, guidelines and procedures.

Remote Access/Off-site Use of IT Resources

- Extreme care should be taken when using remote access, especially in a public area or using a computer that does not belong to you or to the CSCC.
- Sensitive data should not be downloaded to remote or mobile computers/devices.
    - If sensitive data is removed from the CSCC, the user must:
        - Have approval in writing from the study Principal Investigator and encryption is employed. For non-study data the written authorization must be provided by the CSCC Director or Deputy Director.
        - Encrypt data stored on mobile or remote computers/devices.
        - Sensitive data must be encrypted during transmission outside of the CSCC.
- Personal and/or mobile computers/devices must be appropriately secured to prevent loss or theft.
- Remote access sessions to CSCC desktops are set to time out after 30 minutes of inactivity.
- Remote and mobile computers/devices must have all critical O/S patches and up-to-date virus protection. Computers should be set to download and install critical patches and virus definition files automatically.
- Remote and mobile computers/devices must be protected by a strong password that meets CSCC password requirements.
- Blackberry and similar devices must be protected with a 6-character password, a 30-minute time-out, encryption and remote wipe capabilities.
- Do not alter the configuration, including installing software or peripherals, on CSCC equipment unless authorized by the IT manager.
- Use only authorized licensed CSCC software on CSCC equipment unless authorized to do by the IT manager.
- Adhere to all provisions and agreements related to off-site use of computers and accessories and to remote access to any part of the CSCC computer network.
- Protect passwords from access by unauthorized individuals, e.g., do not store passwords in login scripts, batch files, in close proximity to the computer, or elsewhere.

Appropriate Use of the Internet and E-mail

- Use the Internet for business purposes only when on official University time.
- Be aware when navigating through the Internet; you may be moving from an area of controlled access into an area of unknown security controls.
- Report any security incidents to the appropriate officials.
- Do NOT send sensitive information via e-mail or fax, unless encrypted. E-mail attachments can be encrypted but the body of a message can not. Faxes cannot be encrypted, so sensitive information should not be sent by fax.
- Protect copyrighted software and information in accordance with the conditions under which it is provided.
- Ensure sensitive information is not transmitted using personal e-mail accounts.

Access Control

Users:

- Grant access to systems and data only to those who have an official need to know.
- Do not use your trusted position and access rights to exploit system controls or access data for any reason other than in the performance of official duties.
- Never share or compromise your password.
- Make alternative provisions for access to information during your absence to avoid the sharing of passwords.

Managers:

- Delete or reassign accounts as soon as users no longer require access or when they no longer have appropriate approval.
- Plan for disaster recovery and contingency situations.
- Determine access levels based on the user's duties and need to know.

Information Technology (IT) service providers:

IT service providers include (but are not limited to): system administrators, computer operators, system engineers, network administrators, LAN server administrators, those who have access to change control parameters for equipment and software, database administrators, those who control user passwords and access levels, and troubleshooters/system maintenance personnel. IT service providers must:

- Restrict system access to those persons needed to perform assigned duties.
- Ensure system users are aware of their responsibilities regarding access security.
- Plan for disaster recovery and contingency situations.
- Be certain proper software access controls are in place to ensure the security, integrity and privacy of data.
- Set passwords for new accounts per the CSCC Password Policy.
- Set expiration dates for accounts and passwords per the CSCC Password Policy.
- Delete or reassign accounts as soon as users leave the CSCC or when they no longer have appropriate approval.

Selecting Passwords:

The objective when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you have chosen. This leaves him/her no alternative but a brute force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try millions of passwords per second, would require many years to complete.

What Not to Use

- Don't use your login name, e.g., smithj, in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than seven characters.

What to Use

- Do use a password with mixed-case letters if the system password is case-sensitive.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation or combine with alphabetic characters, e.g., $robot2!
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Information Management

General Rules:

- Place only non-sensitive information on publicly accessible systems, including Internet Web pages, e-mail servers, and news groups.
- Ensure that appropriate management officials have approved information for public dissemination.
- Ensure that you do not disclose any sensitive or inappropriate information through the use of public access connections.
- Persistent cookies or fill-in forms should never be used on a site to collect data from users unless pre-approved.
- Ensure that sensitive information sent to a fax or printer is handled in a secure manner.

Backing up Systems:

- Backups should be performed commensurate with the risk and criticality of the data.
- Ensure backups are successful and copies are kept off site.
- Ensure backups are secured in a manner commensurate with the risk and sensitivity of the data.
- Ensure data can be easily restored when necessary.
- Ensure virus protection software is in use and is current.
- Follow up on reported security incidents in a timely manner.
- Destroy backups when no longer needed.

Disposition of Sensitive Resources:

- Hard copies of sensitive information should be destroyed by pulping or shredding.

- Removable media containing sensitive information must be sanitized or the media destroyed.
- When disposing of or transferring a computer system or mobile device, erase all files from the hard drive by using a wipe out utility or destroy the disk.