8 Participant Protections: 8.2 Privacy and Confidentiality	Effective Date: **2/12/2010** Revised: 2/12/2016

In accordance with federal regulations, adequate provisions shall be made to protect the privacy of subjects, and maintain the confidentiality of data, when appropriate, to protect the rights, safety and welfare of participants. Investigators consider issues of privacy and confidentiality in the design and conduct of research. The IRB considers issues of privacy and confidentiality in the review and approval of research.

1.0 Privacy.

When appropriate, federal regulations require research to make adequate provisions to protect the privacy of participants. Privacy refers to an individual's desire to control who has access to him/herself.

The federal regulations define 'private information' as "information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (e.g., a medical or education record)."

1.1 Measures to protect privacy.

In developing strategies for the protection of participants' privacy, consideration should be given to:

- The methods used to identify and contact potential participants.
- The settings in which an individual will be interacting with an investigator. For example, persons may not want to be seen entering a place that might stigmatizing them, such as a pregnancy counseling center that is clearly identified as such by signs on the front of the building.
- The appropriateness of all personnel present for research activities.
- The methods used to obtain information about participants.
- The nature of the requested information.
- Information that is obtained about individuals other than the "target participants," and whether such individual meet the regulatory definition of "human participant" (e.g. a subject provides information about a family member for a survey).
- Privacy guidelines developed by relevant professional associations and scholarly disciplines (e.g., oral history, anthropology, psychology).
- How to access the minimum amount of information necessary to conduct the study.

1.2 Informed Consent.

Unless the IRB has otherwise waived the requirement for informed consent, participants must be informed of the research, the nature of any questions or procedures, and allowed to skip questions. When research obtains private identifiable information about third parties, these individuals would also be considered 'subjects' of the research and informed consent would be required. The IRB may waive informed consent when research will involve use of private records, public observations, or third parties, provided the criteria for waiving informed consent are met. Refer to *9.3 Waiver or Alteration of Informed Consent Requirements* for more information.

1.3 IRB Review considerations.

Federal regulations require the IRB to ensure that the research has adequate provisions to protect the privacy of participants, when appropriate. Refer to *7.2 Criteria for IRB Approval* for more information. Requests for a waiver of informed consent may be considered by the IRB, and approved if all requirements are met and it will not violate the rights of participants. Refer to *9.3 Waiver or Alteration of Informed Consent Requirements* for more information.

1.4 Online communities or sites.

Research involving collection of information and/or recruitment of participants via online communities or websites may also involve privacy concerns. Researchers should be cognizant of what constitutes a public vs. private space. Research projects must consider policies of the online community or site, which may restrict access to their members, use of postings, blogs or discussion groups. When recruitment of individuals would identify them as possessing a stigmatizing or embarrassing condition, or otherwise violate their privacy, recruitment notices (sent via email or other methods) should ensure that their identity cannot become known by other individuals.

2.0 Data Storage and Confidentiality.

The IRB reviews the methods to be used to protect confidentiality and ensures that appropriate protections are in place considering the nature of the research, the vulnerability of the participant population, and the risk associated with a breach of confidentiality.

2.1 Measures to protect confidentiality.

Methods to protect participant confidentiality may include, but are not limited to:

- eliminate (i.e., collect **anonymous** data) or minimize collection of direct or indirect identifiers, including signatures,
- store individually identifying data in separate files from the research data,
- de-identify data as soon as possible,
- use participant-generated codes composed of a combination of elements to link separate data sets,
- physical security measures: e.g., locked offices, locked cabinets, securing mobile devices (e.g., laptops, smartphones, tablets, etc.),
- electronic data safeguarding measures: using current IT security standards: e.g., user passwords and authentication, firewalls, anti-virus programs, encryption, isolation from networks, etc. Specific guidelines for the protection of identifiable research data are outlined in the IRB's "Confidentiality and Data Security Guidelines for Electronic Research Data."
- In some cases, a Certificate of Confidentiality may be required to protect sensitive data from forced disclosure to legal authorities.

2.2 Informed Consent.

Unless the IRB has otherwise waived the requirement, informed consent is required and participants must be informed of how their information will be collected, stored and presented within research results. This may include disclosure of:

- How their data will be used,
- who will have access to it,

- what procedures/protections are in place to ensure that only authorized individuals will have access to the information,
- any further data sharing, mandated-reporting or planned disclosures,
- collection, storage, and eventual disposition of audio or video-recordings,
- any other limitations on confidentiality of their information.

2.3 IRB Review considerations.
Federal regulations require the IRB to ensure the research contains adequate provisions to maintain the confidentiality of research data, when appropriate. Refer to *7.2 Criteria for IRB Approval* for more information. Confidentiality procedures should take into account the sensitivity of information collected and the risks associated with a breach of confidentiality. The IRB may consider a waiver of the signature requirement, if that would serve to protect the identity of participants. Refer to *9.3 Waiver or Alteration of Informed Consent Requirements* for more information.

2.4 Mandated reporting.
Certain information (e.g., child or elder abuse/neglect, harm to self or others, reportable diseases or conditions) collected in the course of a research project may be subject to North Dakota mandated reporting requirements. When an investigator anticipates the possibility of obtaining such information, participants and/or their guardians must be informed of the possibility of disclosure of their information to appropriate authorities. Mandated reporters may include, but are not always limited to: physician, nurse, dentist, optometrist, medical examiner or coroner, or any other medical or mental health professional, religious practitioner of the healing arts, schoolteacher or administrator, school counselor, addiction counselor, social worker, child care worker, foster parent, police or law enforcement officer, juvenile court personnel, probation officer, division of juvenile services employee, or member of the clergy. In addition to those individuals required to report, any other person may also report suspected child abuse or neglect, in accordance with ND State law.

2.5 Other laws.
Research may also require compliance with additional federal or state laws governing confidentiality where applicable, e.g., medical records (HIPAA), or academic records (FERPA). Refer to *11.1 Use of Confidential Records* for more information.

DEFINITIONS:
Confidentiality: pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure without permission.

Identifiable: the identity of the subject is or may be readily ascertained or associated with the information; data can be linked to specific individuals either directly or indirectly through coding systems. This would also include some demographic information, or other unique information or key details that would allow individual identification to be deduced (e.g., using internet search engines or other means).

Private information: information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which

has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (e.g., a medical record).

Privacy: having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

Sensitive information: information about an individual that may be harmful or embarrassing to reveal. This may include information about sexual attitudes, preferences or practices, use of alcohol, drugs or other addictive products, illegal conduct, psychological well-being or mental health, private records (e.g., medical or academic records), or other information that, if released, could reasonably be damaging to an individual's financial standing, employability, or reputation.

RELATED TERMS:

Anonymous: no identifiable information exists; individual identity cannot be known or deduced, no possibility of linkage with additional information or future data collection.

Anonymized (de-identified): identifiers were originally collected, but have been irreversibly removed from previously identified samples; individual can no longer be identified or linked with their information.

Coded: 1) identifiable information has been replaced with a number, letter, symbol, or combination thereof (e.g., the code); and 2) a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens.

Protected health information (PHI): Individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103). The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information found in employment records held by a covered entity in its role as an employer.

Personal identifying information (PII): For the purposes of these guidelines, this includes information that identify a person including any or all of the following: (1) names; (2) social security numbers; (3) birthdates; (4) addresses; (5) IP addresses; (6) other data that could reasonably lead to discovering a personal identity.

REFERENCES:

45 CFR 46.111 and 21 CFR 56.111 Criteria for IRB Approval of Research
45 CFR 46.102 and 21 CFR 50.3 Definitions
OHRP Guidance: Written Procedures
OHRP IRB Guidebook, Chapter III, D. Privacy and Confidentiality
Certificates of Confidentiality, National Institutes of Health
'Protecting Study Volunteers in Research', 2nd Ed., Chap. 6, Behavioral Research Issues, C. McGuire Dunn & G. Chadwick, 2002.
'Institutional Review Board Management & Function', Chap. 5-6, Privacy and Confidentiality, R. Amdur & E. Bankert, 2002.
ND Century Code Chapter 23-07 Reportable Diseases
ND Century Code Chapter 50-25.1 Child Abuse and Neglect

Protection of Third-Party Information in Research, National Institutes of Health

RELATED FORMS:
IRB Protocol Form
Report of Unanticipated Problem or Serious Adverse Event

RELATED HRPP SECTIONS:
7.2 Criteria for IRB Approval
7.7 Unanticipated Problems and Serious Adverse Events
8.1 Risks and Benefits
9.3 Waiver or Alteration of Informed Consent Requirements
11.1 Use of Confidential Records

ADDITIONAL GUIDANCE
Confidentiality and Data Security Guidelines for Electronic Research Data