UWM Institutional Review Board Data Confidentiality Guidance

1. Purpose

Based on the regulations of the Department of Health and Human Services (45 CFR 46), the IRB is responsible for ensuring that each human subjects protocol includes adequate provisions for protecting the privacy of subjects and maintaining the confidentiality of study data.

During the review process, the UWM IRB will review the data security and confidentiality plan for each study submission. Loss of confidentiality is a potential risk to research subjects, researchers and the University, so it is important to the IRB and a plan to properly address this risk should be developed by the researcher (s). The level of required safeguards is dependent upon the sensitivity of the data being collected and the ability to link the data to individual subjects.

2. Definitions (for purposes of UWM IRB documents):

a. **Confidentiality** – The process of protecting an individual's identifiable, private information that was collected during research with the assurance that the data will not be disclosed without permission.

b. **Anonymous** – Study data and/or samples that are free of identifying information (including codes) *before* the researcher has access to it.

c. **Coded** – Study data is stored with (1) a unique code that is free of identifying information AND (2) a key to decipher the code exists which allows the study data to be linked to an individual study participant. The key must be stored separately and securely, so that only limited study personnel have access to link the study data to individual subjects. The code should be a unique number/letter that does not include order of enrollment or date of participation or subject initials. Subject identifiers may be collected but are stored separately from study data.

d. **De-identified** – Data that no longer contains identifying information and cannot be linked back to an individual participant (with a code) by the researcher(s) or anyone else. At one time the data may have been identifiable or coded.

e. **Identifiers** – Data that can be used to identify a person. Depending on the size type of the population, identifiers can come in a variety of forms - name, birthdate, Social Security Number, IP address, student ID number, medical record number, other account numbers, mailing address, job title, photographs, etc.

f. **Sensitive Data** – Information that could put a participant at risk of criminal or civil liability or the risk could have social, financial, medical, legal, employment related, or reputation impacts if a breach would occur. Some examples include research on illegal drug use or sexual practices, genetic research, research on stigmatizing diseases such as HIV, etc.

3. Data Confidentiality Plan

The IRBManager Protocol Form and Continuing Review Form include several questions to allow researchers to describe their data confidentiality plan to the IRB. Please consider the following when preparing your data confidentiality plan:

a. Collect only the information necessary to conduct the study. Information such as birthdate is generally considered an identifier, so when possible ask age or birth year rather than birthdate.
b. Remove/destroy subject identifiers or link between subject ID and identifying information as soon as possible.
c. Safeguards should be in place for data storage (see below).
d. If sensitive data are stored on portable devices (i.e. laptops, USB drives, recording devices, etc.), the device and/or files must be encrypted.
e. If data are shared, you must specify whom it will be shared with and it must be done using secure transmission methods.
f. Cloud Based storage/sharing programs (DropBox, GoogleDocs, etc.) without UWM approved contracts may put your data and the university at risk. Therefore, they cannot be approved by the IRB for use with sensitive and/or identifiable data.
g. Contact IT personnel in your department/division/school for assistance and advice on how to securely store data.
h. Review the recommendations from UITS Security Office and be aware that they are available to offer advice and/or risk assessments: http://uwm.edu/itsecurity/

4. Data Safeguards recommended by the IRB to Protect Confidentiality of Data

a. Electronic Data Safeguards
    i. Storage using a secure UWM Network
    ii. Password protected computer
    iii. Encryption
    iv. Data stored on non-networked computer (with password protection and/or encryption)
    v. Recording data anonymously
    vi. De-identifying data
    vii. Recording data with a code and the key is stored separately
b. Hardcopy Data Safeguards
    i. Locked office and/or file cabinet
    ii. Recording data anonymously
    iii. De-identifying data
    iv. Recording data with a code and the key is stored separately

5. Data Breach

a. If there is a possibility of a data breach involving data from an IRB approved study, the PI must submit a reportable event form to the UWM IRB within 30 days of the event. In addition, the incident should also be reported to the PI's supervisor and the Information

Security Office (infosec.uwm.edu or 414-229-1100). Examples of a data breach may include a known or potential loss of data, including:

i. Theft or loss of any non-encrypted device containing study data.
ii. Compromised account, server or computer containing study data.
iii. Accidental disclosure (i.e. sending data to the wrong person).

b. After review of the event, the IRB may require notification to study participants, the funding agency, UWM Legal, UWM Data security Office, and/or other applicable parties.
c. Researchers should be aware that a data breach may involve fines, cost to notify participants and set up credit monitoring, and required reporting to outside funding agencies and/or the public.