HUMAN RESEARCH PROTECTIONS PROGRAM
UNIVERSITY OF MICHIGAN

Guidance: Protecting Participant Privacy and Maintaining Confidentiality of Data

Introduction

In order to approve research, federal regulations require the IRB to determine, when appropriate, that there are adequate provisions to protect the privacy of participants and to maintain the confidentiality of data. See 45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7).

"Privacy" refers to the willingness of research participants to allow access to themselves and their information. "Confidentiality" refers to the agreement between the researcher and participants on how the participants' identifiable private information will be managed and used.

The purpose of this document is to provide additional guidance for the U-M IRBs and researchers regarding considerations for protecting the privacy of participants and maintaining the confidentially of data in the review and approval of human research.

Researcher Responsibilities

Researchers must include a plan to protect participants' privacy and confidentiality in the eResearch application, protocol or other documents submitted to the IRB. The plan should take into account:

- The proposed participant population;
- The proposed recruitment methods;
- The sensitivity of information collected; and
- The method of data collection.

Researchers are responsible for adhering to the privacy and confidentiality protections as outlined in their IRB approved application.

IRB Evaluation of Proposed Privacy and Confidentiality Protections

The IRB reviews the researcher's plan to protect participants' privacy and maintain confidentiality of data, utilizing regulatory, institutional and internal policies, procedures, and guidance, including, but not limited to:

- Code of Federal Regulations/Protection of Human Subjects (45 CFR 46)
- Food and Drug Administration (FDA)/Protection of Human Subjects (21 CFR 56)
- Health Insurance Portability and Accountability Act (45 CFR Parts 160 and 164)
- University of Michigan Website Guidance for Sensitive Human Subjects Data

Issues and points of interest the IRB considers when reviewing privacy protections include all of the following:

- The research setting, participant population, the manner in which participants will be approached and enrolled, and inclusion of any un-consented individuals about whom the primary participants will provide information;
- Whether the protocol proposes an invasion of privacy through observation or intrusion into situations where participants would otherwise have a reasonable expectation of privacy; and

- Where there is a risk that privacy may be compromised, the IRB will evaluate:
  - Whether reasonable people might be offended by the invasion of privacy;
  - Whether the research can be redesigned to avoid the possible invasion of privacy;
  - Whether the importance of the research objective justifies the invasion of privacy;
  - Whether the participant will be informed of the invasion of privacy, its implications, and available protections; and
  - Whether documentation of consent should be waived in order to protect participant privacy.

Issues and points of interest considered when reviewing confidentiality protections include all of the following:

- The research setting, participant population, the manner in which participants will be approached and enrolled, where private information will be collected, the nature of information, who will collect, receive and use the information and inclusion of any un-consented individuals about whom the primary participants will provide information or for whom the researchers will obtain information through record review or chart abstraction;
- Whether appropriate permission is sought for access to records when reviewing existing records for participant selection or to abstract data;
- Whether the protocol proposes the collection of sensitive and identifiable individual information;
- Where the research includes the collection of sensitive and identifiable individual information, the IRB will evaluate:
  - Whether adequate data management and security provisions have been identified to protect the confidentiality of the data through coding, destruction of identifying information, limiting access to the data, and any other methods that may be appropriate, given the context of the study;
  - Whether the disclosure of the data might place the participant at legal, social, reputational, employability, or insurability risk;
- Where compelled disclosure of the data might place participants at risk, and whether a Certificate of Confidentiality (CoC) should be sought to protect the researcher from disclosure of the data under subpoena or other legal process, unless a CoC is already provided by the terms and conditions of funding;
- Where accidental disclosure of the data might place participants at risk, whether data management procedures ascribe to institutional policies and IRB guidance for appropriate and required data security measures;
- Whether disclosures to participants about confidentiality risks and protections are adequate; and
- Whether documentation of consent should be waived in order to protect confidentiality.

Resources

Certificates of Confidentiality

U-M Safe Computing: Safely Use Sensitive Data

IRB-HSBS Guidance: Data Security Guidelines