Department: **UAMS Institutional Review Board**
Policy Number: **13.1**
Section: **Confidentiality**
Effective Date: **July 31, 2002**
Revision Date: **June 10, 2004; January 24, 2011; February 15, 2016; August 28, 2020**

SUBJECT: Confidentiality Protections

POLICY
In its reviews, the IRB shall consider whether research subjects' identifiable private information is appropriately protected with regard to its collection, storage, use, and sharing, as applicable.

DEFINITIONS
Certificate of Confidentiality: Certificates of Confidentiality (CoCs) protect the privacy of research subjects by prohibiting disclosure of identifiable, sensitive research information to anyone not connected to the research except when the subject consents or in a few other specific situations. They do not prevent research subjects from voluntarily disclosing their own information. Nor does a CoC prevent researchers from disclosing matters such as child abuse or a subject's threatened violence to self or others. However, if a researcher may make such disclosures, the consent form should clearly indicate this possibility.
Information: Data about individuals, including but not limited to data a) collected by accessing previously created data sources; b) collected by interaction with subjects or those acting on behalf of the subject; also includes biospecimens and any information associated with such specimens.
Identifiable Information: Information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.
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/or information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (e.g. a medical record).
Sensitive Information: Information that, if made public or otherwise released, may be embarrassing to the person whose information it is or put them at legal or reputational risk; or may pose other types of risks to the person. Examples include, but are not limited to, information:

- Relating to sexual attitudes or behaviors;
- Relating to the use of alcohol, drugs or other addictive products;
- Pertaining to illegal conduct;
- That, if released, could reasonably be damaging to an individual's financial standing, employability, or reputation within the community;
- That would normally be recorded in a patient's medical record, and the disclosure of which could reasonably lead to social stigmatization or discrimination;
- Pertaining to an individual's psychological well-being or mental health;
- Pertaining to genetic characteristics of the individual or of the individual's blood relatives.

PROCEDURES
A. In its reviews, the IRB will consider whether the data to be accessed, collected, and used for the research are:
    1. Relevant for the proposed research. The IRB may request more information from the study team if some of the information does not appear related to the research question.
    2. Collected or accessed in a manner that adequately protects data confidentiality. Considerations include, but are not limited to:
        a. Whether the data will be accessed or collected in an appropriately protected area
        b. How the data will be recorded (e.g. on paper, a portable electronic device, directly on a protected server behind an institutional firewall)
        c. How the data will be identified (e.g. collected without identifiers; coded, with a key to the code kept separately; directly identified)
        d. Recorded and stored in a manner that minimizes unauthorized access to or sharing of the data
        e. If and when any identifiers will be destroyed
B. The IRB will discuss with the research team if the IRB feels the aims of the research may be accomplished without accessing identifiable information, e.g. through a request for anonymized data from a central database. The IRB may require the investigator to provide a rationale for accessing/using identifiable data when alternatives to such use/access may exist.

C. The IRB and the research team will consider whether a Certificate of Confidentiality is available and appropriate for the research.
   1. Effective October 1, 2017, research commenced or ongoing on or after December 13, 2016, and is funded or supported by the NIH is automatically covered by a certificate of confidentiality. NIH has a process by which investigators on studies funded by other federal agencies or by non-federal funding sources may also request a CoC.
   2. If the study is not automatically covered by a CoC, and the IRB determines confidentiality protections afforded by a CoC are appropriate to the research, the IRB may require the investigator to apply for a CoC.
   3. When research is covered by a CoC, researchers:
      a. May not disclose or provide, in any federal, state, or local civil, criminal, administrative, legislative, or other proceeding, the name of an individual or any such information, document, or biospecimen containing identifiable, sensitive information about the individual created for the research, unless the individual consents to such disclosure/use;
      b. May not disclose or provide to anyone not connected with the research the name of such an individual or any information, document, or biospecimen that contains identifiable, sensitive information;
      c. May disclose information only when:
         i. Required by state, federal, or local laws
         ii. Necessary for the medical treatment of the individual to whom the information or biospecimens pertain
         iii. Made with the consent of the individual to whom the information or biospecimens pertain;
         iv. Made for the purposes of other research that is in compliance with applicable federal regulations and institutional policies governing the protection of human research subjects.
      d. Must inform participants of the protections and limitations of CoCs.
      e. Must ensure, if identifiable, sensitive information is provided to other researchers or organizations, the other researcher or organization must comply with applicable requirements when research is covered by a CoC.

D. The protocol submission in the IRB e-system shall address:
   1. The information required for the IRB to make the determinations in this policy and other relevant policies and regulations pertaining to data confidentiality.
   2. If appropriate, whether the study team has, or will seek, a certificate of confidentiality.

REFERENCES

45 CFR 46.111(a)(7)
21 CFR 56.111(a)(7)
AAHRPP Element II.3.E
AAHRPP Tip Sheet 4, *Confidentiality of Data*