

The National Institutes of Health, or NIH, issue Certificates of Confidentiality to protect sensitive and identifiable information about study subjects against forced disclosure. Certificates of Confidentiality allow members of a study team to refuse to disclose such information in any legal proceeding, whether at the federal, state, or local level.

A study may be eligible for a Certificate if it involves collection of sensitive information and identifying characteristics, and if disclosure would have adverse consequences for subjects, including damage to

- financial standing
- employability
- insurability
- or reputation

Sensitive information includes things like:

- genetic information
- information about a subject's psychological health
- information about a subject's sexual attitudes, preferences, or practices
- information about a subject's substance abuse or any illegal behavior

Identifying characteristics include a subject's:

- name
- address
- Social Security or other identifying number
- fingerprints
- voiceprints
- photographs
- genetic information or tissue samples
- and any other information about a subject that may lead, either directly or by reference to other information, to the identification of that subject

Before NIH will issue a Certificate of Confidentiality, a study must already have IRB approval. Since informed consent documents need to include an explanation of the Certificate, investigators should inform the IRB at the beginning of the application process that they're planning to obtain a Certificate and have included the appropriate language in their consent documents.

## U-MIC TRANSCRIPT

### NIH Certificates of Confidentiality

A Certificate protects the information investigators maintain while the Certificate is in effect, and that information remains protected as long as it is in the possession of the study team. Even sensitive information investigators may already have collected becomes protected once NIH has issued the Certificate.

Certificates of Confidentiality do not reduce all research-related risks and *do not* eliminate an investigator's duty to implement data security measures. Likewise, Certificates do not protect sensitive data against all forms of disclosure. For example, even with a Certificate in place, investigators would still be required to disclose sensitive information for audits or program evaluations conducted by the Department of Health and Human Services, or under the Food, Drug, and Cosmetic Act.

Additionally, a Certificate of Confidentiality will not protect sensitive information against voluntary disclosure, as in instances of child abuse, threats of physical harm, reportable communicable disease, as well as a subject's own disclosure. Investigators should specify in their informed consent documents which voluntary disclosures are not protected by the Certificate.

NIH's Certificates of Confidentiality protect subjects' sensitive, identifiable information from forced disclosure, such as by court order or subpoena.

For more information about Certificates of Confidentiality, visit NIH's web site or contact the IRB.

*Posted: 5/30/12*