SOP 1.3.4 Certificate of Confidentiality and Privacy Certificates

General Description:

Investigators generally do not disclose identifying information about research subjects to individuals or entities outside of the research team. However, there may be occasions where, because of a court or administrative agency subpoena, the investigator may be required to disclose records of a subject's participation in a research study that could include name, address, and medical history.

Certificates of Confidentiality (CoC) are issued by the National Institutes of Health (NIH) to protect identifiable research information from forced disclosure. The Department of Justice (DOJ) requires privacy certificates (PC) on all studies funded by DOJ that collect identifying information. Both CoCs and PCs allow the investigator and others who have access to research records to refuse to disclose identifying information on research participants in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. By protecting researchers and institutions from being compelled to disclose information that would identify research subjects, COCs and PCs help assure confidentiality and privacy to research subjects. As long as a COC or PC is in place when a subject enrolls in a study, information identifying the subject will never be disclosed unless the subject volunteers it or in certain specific circumstances, the investigator volunteers it.

Researchers may obtain CoCs provided that a determination is made by the IRB and/or the issuing agency that the research is of such a sensitive nature that protection is necessary to perform the research (an example of this might be collecting data pertaining to illegal behaviors). The National Institutes of Health and other HHS agencies issue CoCs. All research collecting identifying information and funded by DOJ requires a PC.

COCs are valid from the date of issue to the date of study expiration, and if the research is not completed by the termination date of the certificate, the recipient must make a written application for an extension. A CoC or PC is not transferable from one study to another. Any significant changes to the protocol, study personnel, or the test article to be administered requires notification to the issuing agency by the submission of an amended application.

Once a subject enrolls in a study in which a CoC or PC is in place, the protection afforded by the certificate is permanent and information identifying that subject will never be disclosed unless it is volunteered by the subject or the investigator for certain urgent issues, or it expires.

Procedures:

1. **Identify the need for a Certificate.** A Certificate should be requested when a research project is collecting information from or about subjects that is identifiable and sensitive in the case of CoC or simply identifiable in the case of a PC. This may be at the time of the initial IRB review. In some cases, the need may arise when a researcher modifies an IRB-approved study to include identifiable or sensitive information.
    a. The IRB can require the researcher to obtain a CoC if, by the IRB's assessment, the sensitivity and risk associated with the data collected would benefit under the purview of the CoC. If the Mason IRB determines that a CoC is necessary to minimize risks to

human subjects, the final approval of the study will not be granted until such a CoC is obtained.

b. The researcher can decide to apply for a CoC if it is believed that one is necessary.
c. Federal agencies can require a researcher to obtain a CoC or PC at any time.

2. **Researchers submit a request for a CoC.** A request for a CoC or PC must be made for a particular study to the agency responsible for the funding, and is not transferable to any other study. Any person engaged in research in which identifiable and sensitive information is gathered from human research participants (or any person who intends to engage in such research) may apply for a CoC.
    a. If the research is not supported by a federal agency that issues Certificates, then the researcher may apply for a Certificate through the NIH Institution or Center that funds research in the same or a similar scientific area.
    b. The Food and Drug Administration (FDA) issues a CoC for non-NIH-funded studies that involve an Investigational New Drug (IND) application or an Investigational Device Exemption (IDE).
    c. The DOJ issues PCs for all studies funded by DOJ where identifiers are collected.

3. **Researchers must submit the CoC or PC for review.** The CoC application requires the inclusion of Assurances which are signed by the Principal Investigator and the IO. These Assurances document that the institution will use the CoC to protect against compelled disclosure and defend the authority of the Certificate against legal challenges; they also indicate what participants are to be told about the CoC. Please see details at: http://grants.nih.gov/grants/policy/coc/appl_extramural.htm. Contact Mason's IRB office and the office staff will obtain the IO's signature. PCs should be submitted to the IRB office for review prior to submission to DOJ.

4. **Submit the CoC with the IRBNet Application.**
    a. A copy of any CoC/PC and/or any amendments to such an application must be submitted to the Mason IRB.
    b. The IRB application and attachments must describe all of the situations in which (and to whom) the researcher might voluntarily disclose identifying information about a subject. Subjects should be advised about the exceptions to the protections the certificate offers, and should be adequately informed during the consent process.
        i. Researchers may choose to use the template language provided by NIH or DOJ. Researchers may also create their own language, but it must contain the following elements.
            1. Description of the protections and limitations of the Certificate, including the circumstances in which the researchers plan to voluntarily disclose identifying information about the subjects (e.g., audits; child abuse; harm to self or others; etc.).
            2. Statement that the Certificate does not prevent the subject or subject's family from voluntarily disclosing information about the subject or

involvement in the study, or from authorizing others to receive such information.

3. The language about confidentiality and data security that is routinely included in consent forms should be consistent with the protections of the Certificate.

5. **IRB Review.** Upon receipt of the materials, the Mason IRB will follow the review procedures outlined in the applicable SOPs. As part of its review of a new application or a Modification, the IRB may consider whether a CoC/PC is appropriate. The IRB has the authority to require the researcher to apply for a Certificate.
    a. IRB approval cannot be granted until the Certificate has been obtained and provided to the IRB.
    b. The consent form will be reviewed to ensure the purpose, protections, and any limitations are adequately disclosed.
    c. The IRB staff and members will verify the expiration date of the CoC at the time of continuing review.

6. **Filing.** Any CoC/PC correspondence regarding it will be maintained with the study file in IRBNet.

Related Forms, Guidance, and SOPs:

- NIH Certificates of Confidentiality; available at: http://grants.nih.gov/grants/policy/coc/index.htm
- DOJ Privacy Certificates; available at: http://www.nij.gov/funding/humansubjects/pages/privacy-certificate-guidance.aspx.
- OHRP Guidance on Certificates of Confidentiality; available at: http://www.hhs.gov/ohrp/policy/certconf.html.
- Certificates of Confidentiality Contacts at NIH and Other DHHS Agencies that issue Certificates; available at: http://grants2.nih.gov/grants/policy/coc/contacts.htm
- 45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)
- 45 CFR 46.116(a)(5) and 21 CFR 56.111(a)(5)
- 28 CRF 22
- 42 USC 3789g
- 28 CFR 46

Responsibility:

Execution of SOP:
Principal Investigator
Study Team Members
IRB Staff
Institutional Official

Approval and Version History:

Please contact irb@gmu.edu if you have any questions about this policy or the version and approval history.

Date First Effective:	February 24, 2016
Revision Date:	[DATE]
Current Version #:	1

Approved By	Title and Division	Date Approved
Aurali Dade	Assistant Vice President, Office of Research Integrity and Assurance	February 24, 2016
Greg Guagnano	IRB Chairperson	February 24, 2016