PROTECTION OF CONFIDENTIAL DATA IN HUMAN SUBJECTS RESEARCH

POLICY

Researchers who will collect and/or have access to restricted data including protected health information (PHI) and any other information that the IRB determines is highly sensitive during the course of human subjects’ research projects will assure the privacy of individuals and the protection of data collected during the conduct of their studies and after the study is closed in keeping with university information security (data protection) policies as well as state and federal laws and regulations; including but not limited to HIPAA and HITECH. Restricted data includes any information that can be identified with or linked to an individual participating in research including any special code number given to the individual for purposes of research if a key exists that can link with the number, or any information specific enough to identify the participant. HIPAA outlines 18 specific identifiers:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
Human Research Protection
Program Policy

15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data)

The method the researcher chooses to protect the data must comply with all applicable federal regulations and university policy and be described in the IRB protocol. The IRB will not approve a research study unless the following requirements are met:

THE PROTOCOL SUBMISSION FORM

Restricted data must be secured in a manner that is consistent with university policies and applicable regulations. If the data are paper records, the researcher will describe the measures used to protect it (e.g. records must be in a locked file cabinet, within a restricted area, and those who have access must be identified). If participants are assigned ID numbers requiring a code to link the identifiers to personally identifiable information, the location of the code and the individuals who have access to it must be included in the protocol. If the data are electronic, they must be secured in compliance with UC data protection policies (current versions are available online from the Office of Information Security website, www.uc.edu/infosec/policies.html).

1. The IRB will determine whether the method the researcher describes in the protocol and consent form are adequate to protect the confidentiality of the data and may monitor the study to assure compliance.

2. For those projects where the identity or other information about participants is intended to be published as part of the research, the protocol will specify what information is intended to be public and that research participants will be fully informed that the data will be made public. The researcher will describe what, if any measures need to be taken to protect data prior to publication.

THE INFORMED CONSENT PROCESS

The informed consent process and the Informed Consent Document shall inform participants of the persons, offices, or agencies that have access to identified data or data that can be linked to a participant.
1. Those with access to identified or identifiable data shall include the researchers engaged in the study, the sponsor of the study, regulatory and accrediting agencies, the HRPP staff and university employees/agents whose job responsibilities include defending the university and its employees against claims, whose job responsibilities include monitoring compliance with laws, rules, regulations, or university policy, investigating non-compliance, and any attorney, auditor, consultant, law enforcement agent, or accountant engaged by these university employees to fulfill these responsibilities. For studies to be conducted at the Veterans’ Affairs Medical Center (VAMC), the Informed Consent Document will state that the VAMC and its agents shall have access to the data.

2. The researcher may not give access to the data to anyone not listed in the Informed Consent Document unless the participant consents in writing to having his or her data shared.

3. If university employees or their agents listed above request identified or identifiable data in order to defend the university against claims, to monitor or audit studies, or to investigate allegations of non-compliance, all identifiers will be redacted unless it is not possible for the university employee or agent to fulfill their job responsibility without identified data.

4. The Informed Consent Document shall contain a phone number or email address for participants to use who are concerned about the conduct of the study or have a complaint about their participation in the study, including the unauthorized release of their data.

5. If the unauthorized release of confidential data presents more than minimal risk to individuals participating in research, the consent form shall discuss what the risks of breach of confidentiality are, such as social stigma or loss of employment, and shall further state what follow-up care, counseling, social support services, or other intervention is available to the participant.

SECONDARY ANALYSIS OF DATA

In most cases, information must have been included in the original consent form that describes the potential future use of the data, to allow the subjects to provide consent for these secondary analyses. However, under appropriate conditions and with IRB approval the secondary use may
be allowed without consent provided it meets the requirements for waiver of informed consent as described in Policy II.01 Obtaining Informed Consent in Human Subjects Research.

If consent was not obtained for this secondary analysis, the Board will review the study and determine if the secondary use of the data should be allowed without consent. Factors that would be considered during this review include; whether the secondary use is similar to those for the original use, is the use minimally intrusive, whether the activity meets the criteria for waiver of informed consent, if the data are deidentified, and that appropriate confidentiality protections can be assured.

If the original informed consent stated that data would not be used for any purposes other than those described in the consent form, secondary use of data will not be allowed without informed consent from the subjects.

CERTIFICATE OF CONFIDENTIALITY

Investigators whose studies involve more than minimal risk of disclosure of confidential information may obtain a Certificate of Confidentiality from the Department of Health and Human Services. The Certificate protects research participants from risk of disclosure of confidential information pursuant to subpoenas in civil or criminal actions. See http://www.grants.nih.gov/grants/policy/coc/appl_extramural.htm?Display=Text

Applicable Regulations, Documents:

UC Rule 10-5-20
UC Data Protection (Information Security) Policies
45 CFR 46.111 (a)(7)
45 CFR 160, 162, and 164
5 USC § 552
18USC § 2510-2522
42 USC § 300jjj et seq.
42 USC § 17921 et. Seq.
ORC §1347.15
111 PL5
1349.19
H.R. 145
Public Law 107-347
Human Research Protection Program Policy

<table>
<thead>
<tr>
<th>Adoption Date</th>
<th>Created By</th>
<th>Date of Revision</th>
<th>Revised By</th>
<th>Summary of Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2005</td>
<td>C. Fabby</td>
<td>06/2014</td>
<td>M. Linke</td>
<td>Revise to reflect changing regulations</td>
</tr>
</tbody>
</table>

Date Adopted       June 2014       Signature       signature on file