Policy Number 24
Title: Subject Privacy, Protection of Confidentiality and Data Security
Date of Last Revision: 03/30/09; 10/11/10; 05/10/15; 03/03/16; 05/01/16; 09/27/17; 10/19/17; 06/13/18

Policy:
It is the policy of the UC Irvine (UCI) Institutional Review Board (IRB) to consider whether adequate provisions exist for the protection of subject privacy, the maintenance of confidentiality of identifiable research data and data security. In order to ensure that risks related to a potential breach of confidentiality are minimized, all human subjects research protocols must have acceptable, effective, and documented procedures for the protection of identifiable and/or confidential information collected or examined for research purposes. The UCI IRB, in its role as the Privacy Board for Research, also ensures that research data be used, stored and/or disclosed according to current HIPAA regulations.

I. Research Design

Research should be designed to minimize the intrusion on privacy to no more than is necessary and the confidentiality of the data obtained during the research should be protected throughout the project as well as after the research is completed.

II. Protection of Privacy

Privacy refers to a person's desire to control the access of others to themselves. For example, persons may not want to be seen entering a place that might stigmatize them, such as a pregnancy counseling center clearly identified by signs on the front of the building. The evaluation of privacy also involves consideration of how the researcher accesses information from or about potential participants (e.g., recruitment process). IRB members consider strategies to protect privacy interests relating to contact with potential participants, and access to private information.

III. Identification of Research Records

A. Protocols should be designed to minimize the need to collect and maintain identifiable information about research subjects.
B. If possible, data should be collected anonymously or the identifiers should be removed and destroyed as soon as possible.
C. When it is necessary to collect and maintain identifiable data, the IRB will ensure that the protocol includes the necessary safeguards to maintain confidentiality of identifiable data and data security appropriate to the degree of risk from disclosure.

IV. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

A. HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996.
B. The intention of HIPAA is to protect patients from inappropriate disclosures of "Protected Health Information" or "Personal Health Information" (PHI) that can cause harm to a person's insurability, employability, etc.
    1. PHI is information that can be linked to a particular person and that is created, used, or disclosed in the course of providing a health care service (i.e., diagnosis or treatment).
    2. Examples of PHI include, but are not limited to, the following:

a. Names;
b. All geographic 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 are changed to 000.
c. 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;
d. Telephone numbers;
e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;
l. Vehicle identifiers and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators (URLs)
o. Internet Protocol (IP) address numbers;
p. Biometric identifiers, including finger and voice prints;
q. Full face photographic images and any comparable images; and
r. Any other unique identifying number, characteristic or code.

C. The Privacy Rule is a nickname for DHHS' regulation, "Standards for Privacy of Individually Identifiable Health Information," applicable to entities covered by HIPAA. In May 2002, the Board of Regents designated the University of California as a HIPAA hybrid covered entity and determined that UC would be a Single Health Care Component for the purposes of complying with the HIPAA Privacy Rule.

D. HIPAA affects only that research which uses, creates, or discloses PHI. Researchers often have legitimate needs to use, access, and disclose PHI to carry out a wide range of health research studies. The Privacy Rule protects PHI while providing ways for researchers to access and use PHI when necessary to conduct research.

E. The IRB acts as a Privacy Board for Research per HIPAA to review the use/disclosure of PHI and to determine whether participants should sign an "Authorization" (an addendum to the consent to participate in research) or if a Waiver of HIPAA Authorization (roughly analogous to a Waiver of Consent under the Common Rule) may be granted.

F. Waivers of HIPAA Authorization: Although it is always preferred to get permission to use an individual's PHI, HIPAA permits research using PHI without obtaining permission (called “Authorization”). In order to waive HIPAA Authorization, the IRB must determine that the study meets all of the following criteria:
1. The use or disclosure of PHI involves no more than minimal risk;
2. Granting of the waiver will not adversely affect privacy rights and welfare of the individuals whose records will be used;
3. The protocol could not practicably be conducted without a waiver;
4. The protocol could not practicably be conducted without use of PHI;

5. The privacy risks are reasonable relative to the anticipated benefits of research;
6. An adequate plan to protect identifiers from improper use and disclosure is included in the research proposal;
7. An adequate plan to destroy the identifiers at the earliest opportunity, or justification for retaining identifiers, is included in the research protocol;
8. The research plan includes written assurances that PHI will not be re-used or disclosed for other purposes; and
9. Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

G. If the IRB permits a waiver of HIPAA Authorization, the justification is documented in the protocol file and, if applicable, the IRB meeting minutes.

H. Limited Data Set (LDS) - A limited set of identifiable information in which most of the identifiers for the individual, the individual's relatives, employers and household members have been removed.
1. The only allowable PHI identifiers are:
   a. 5-digit zip code (4 digit extension is not allowed)
   b. Full dates of birth or death
   c. Full date(s) of service (admission and discharge)
   d. Geographic subdivision (other than street address)
2. For direct access to the medical record to obtain a LDS, a waiver of HIPAA Authorization is required.
3. Investigators may be required to sign a Data Use Agreement through UCI Sponsored Projects for data received by UCI to give assurance that the information will be protected. Similarly, for data sent outside of UCI, a Data Use Agreement may be required through the Office of Research Oversight.

V. Protection of Confidentiality and Data Security

A. A guiding principle of research involving human volunteers is that a participant's privacy must be respected and confidentiality of person-identifiable data must be preserved.

B. Access to research data should be based on a "need to know" and "minimum necessary" standard.

C. Since a breach of confidentiality may present a risk of harm to subjects (e.g., as when the researcher obtains information about the participants that would, if disclosed by the researcher, jeopardize their employment, social standing, or lead to criminal or civil prosecution), the IRB carefully considers whether there is an appropriate plan to protect the confidentiality of research data (e.g., coding data, removal of identifying information, limiting access to data, use of Certificates of Confidentiality or other methods as appropriate).

D. The IRB also evaluates the following:
1. Whether methods used to identify and recruit potential participants protect subject privacy;
2. Whether the consent form fully discloses the extent to which confidentiality will be protected and the potential risks to subject privacy/confidentiality; and
3. Whether the appropriate physical safeguards are in place for protecting confidentiality of research data and data security (e.g., maintenance of records in locked files, separation of person-identifiable data from study data and/or use of unique study ID numbers in place of identifiers, etc.)

E. When applicable, the IRB ensures that prospective subjects are informed of the following in the consent form:
1. Whether records identifying the subjects will be maintained;
2. How the subject identifiable data will be maintained to ensure confidentiality;

3. How long the subject identifiable data will be maintained; and
4. Who will have access to the data.
    a. When FDA-regulated products are being studied; subjects are informed that the FDA may have access to their study records to protect their safety and welfare. Any information derived from the research project that personally identifies the subject will not be voluntarily released or disclosed by these entities without the subject's separate consent, except as specifically required by law; and
    b. Research records provided to authorized, non-UCI entities will not contain identifiable information about the subject.
5. Publications and/or presentations that result from the study will not include identifiable information about the subject.

VI. Certificates of Confidentiality

A. Certificates of Confidentiality are issued by the DHHS' National Institutes of Health (NIH) to protect the privacy of research subjects by protecting researchers and institutions from being compelled to release information that could be used to identify subjects with a biomedical, behavioral, clinical or other research study.

B. Section 2012 of the 21st Century Cures Act, enacted December 13, 2016, enacts new provisions governing the authority of the Secretary of Health and Human Services (Secretary) to protect the privacy of individuals who are the subjects of research, including significant amendments to the previous statutory authority for such protections, under subsection 301(d) of the Public Health Service Act.

1. Specifically, the amended authority requires the Secretary to issue to investigators or institutions engaged in biomedical, behavioral, clinical, or other research in which identifiable, sensitive information is collected ("Covered Information"), a Certificate to protect the privacy of individuals who are subjects of such research, if the research is funded wholly or in part by the Federal Government.
2. The authority also specifies the prohibitions on disclosure of the names of research participants or any information, documents, or biospecimens that contain identifiable, sensitive information collected or used in research by an investigator or institution with a Certificate.
3. Certificates of Confidentiality are issued to institutions or universities where the research is conducted. Any investigator or institution for which identifiable sensitive information is shared is also subject to disclosure restrictions.
4. The Certificates of Confidentiality protects the privacy of subjects by limiting the disclosure of identifiable, sensitive information. Under the new policy, disclosure is not up to the discretion of the investigator. Disclosure is only permitted in the following circumstances:
    a) if required by other Federal, State, or local laws, such as for reporting of communicable diseases
    b) if the subject consents; or
    c) for the purposes of scientific research that is compliant with human subjects regulations.
5. If the research is not federally funded, the Secretary may issue a Certificate to an investigator or institution engaged in such research, upon application.

C. Because of the protections it affords, the IRB may require researchers to acquire a Certificate of Confidentiality as a condition of approval for research involving sensitive matters. Examples of sensitive research activities include, but are not limited to, the following:

1. Collecting genetic information;
2. Collecting information on psychological well-being of subjects;

3. Collecting information on subjects' sexual attitudes, preferences or practices;
4. Collecting data on substance abuse or other illegal risk behaviors;
5. Studies where subjects may be involved in litigation related to exposures under study (e.g., breast implants, environmental or occupational exposures).

D. Not eligible for a Certificate are activities that are:
1. Not research;
2. Not collecting personally identifiable information;
3. Not reviewed and approved by the IRB as required by these guidelines; or
4. Collecting information that if disclosed would not significantly harm or damage the participant.

E. In general, certificates are issued for single, well-defined research protocols rather than groups or classes of protocols.
1. In some instances, they can be issued for cooperative multi-site protocols. A coordinating center or "lead" institution designated by the NIH program officer can apply on behalf of all institutions associated with the multi-site project.
2. The lead institution must ensure that all participating institutions conform to the application assurances and inform participants appropriately about the Certificate, its protections, and the circumstances in which voluntary disclosures would be made.

F. A Certificate of Confidentiality protects all information identifiable to any individual who participates as a research subject (i.e., about whom the investigator maintains identifying information) during any time the Certificate is in effect.

G. Generally, Certificates are effective on the date of issuance or upon commencement of the research protocol if that occurs after the date of issuance.
1. The expiration date usually corresponds with the completion of the study.
2. The Certificate states the date upon which it becomes effective and the date upon which it expires.
3. Although an extension of coverage must be requested if the research extends beyond the expiration date of the original Certificate, the protection afforded by the Certificate is permanent (i.e., all personally identifiable information maintained about participants in the protocol while the Certificate is in effect is protected indefinitely).

H. Limitations and Exceptions
1. Subjects may authorize in writing the investigator to release their information to insurers, employers, or other third parties. In such cases, researchers may not use the Certificate to refuse disclosure.
2. Additionally, while Certificates protect against involuntary disclosure, they do not protect subjects against voluntary disclosure of information by the subject (e.g., when research subjects voluntarily disclose their research data or information to their physicians or other third parties).
3. In accordance with California law, researchers are not prevented from the voluntary disclosure of matters such as child abuse, elder abuse, reportable communicable diseases, or subject's threatened violence to self or others.
4. Finally, Certificates do not authorize researchers to refuse to disclose information about subjects if authorized DHHS personnel request such information for an audit or program evaluation.
    a. Researchers cannot refuse to disclose such information if it is required to be disclosed by the Federal Food, Drug, and Cosmetic Act.

VII. Use of State Death Records

A. Effective January 1, 2003, California law requires local IRBs to review research using California state death data files containing personal identifying information (i.e., state issued death certificates and indices).

1. This law is more restrictive than federal human research protection regulations, which govern use of living humans or identifiable data about living humans.
2. The state requires IRBs to protect information about deceased persons as carefully as information about living persons.

B. In order for an IRB to permit such a study, the state requires that the researcher have a "valid scientific interest."

C. State death records do not fall under the federal exemption from IRB approval for research on publicly available existing data (as these records are no longer publicly available); therefore such studies may require expedited review.

References:

21 CFR §56.111(a)(7)
21 CFR 50.25(a)(5)
21 CFR 56.110
21 CFR 312.68
21 CFR 812.145(c)
45 CFR 46.110
45 CFR 46.116(a)(5)
45 CFR §46.111(a)(7)
45 CFR 164.514(e)
45 CFR 528(a)(viii)
California Health and Safety Code 102231
Child Abuse and Neglect Reporting Act, Cal. Penal Code, Section 11165 et seq.; Elder Abuse and Dependent Adult Civil Protection Act, Cal. Welfare. & Inst. Code, Section 15601 et seq.; Reports of Injuries, Cal. Penal Code, Section 11160 et seq.
National Institutes of Health, Office of Extramural Research, "Certificates of Confidentiality: Background Information", Web Posting: 7/22/2003
OHRP Compliance Activities: Common Findings and Guidance #3, #4
Section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)).
Privacy Rule of the Health Insurance Portability and Accountability Act of 1996, Section 64.514.
Public Health Service Act, S 301(d), 42 U.S.C. s 241 (d), as added by Pub. L. No. 100-607, S 163 (November 4, 1988).
"Checklist for IRBs to Use in Verifying that Human Subject Research Protocols Are in Compliance with DOE Requirements"
DOJ: 28 CFR 22, 28 CFR 512.8,11,12,13,15
UCOP HIPAA Glossary: http://policy.ucop.edu/doc/1110170/HIPAA-11
UCOP HIPAA and Research: http://policy.ucop.edu/doc/1100616/HIPAA%2014

Procedure Number: 24.A
Title: Procedure to Ensure Subject Privacy and the Protection of Confidentiality

Procedure:
This procedure outlines the responsibilities of the UC Irvine (UCI) Institutional Review Board (IRB) and guidance to Investigators to assure that all studies conducted at the UC Irvine Medical Center (UCIMC) ensure subject privacy and confidentiality of data, and are in compliance with the HIPAA regulations.

I. Lead Researcher (LR) Responsibilities

A. LRs should make every effort to reduce the likelihood of a potential breach in confidentiality; especially when a breach of research data could reasonably place subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, insurability, or reputation. The LR should consider the following methods of securing data when designing his/her research:

1. Collect only the minimum necessary subject identifiers.
2. Remove/destroy subject identifiers as soon as they are no longer needed. See Procedure 5.B for research record retention requirements.
3. Limit physical access to any area or computer that contains subject identifiers.
4. Limit electronic access to any computer that contains subject identifiers.
5. Avoid storing subject identifiable data on portable devices (such as laptop computers, digital cameras, portable hard drives including flash drives, USB memory sticks, iPods or similar storage media) as these devices are particularly susceptible to loss or theft. If there is a necessity to use portable devices for initial collection of subject identifiers, the data files should be encrypted, and subject identifiers transferred to a secure system as soon as possible.
6. Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location.
7. If subject identifiers will be retained in the data files because of the specific needs of the research study, additional justification must be provided by the Researcher to justify retention.
8. Use only secure modes of transmission of data; subject identifiers submitted over a public network should be encrypted.
9. Review the UCI Office of Information Technology (OIT) website for additional recommendations on how to best secure confidential research data.

B. In the Confidentiality section of the IRB Protocol Narrative, LRs must address the method of collecting, recording, coding and maintaining data, as well as specify who will have access to the data and at what point subject identifiable data will be de-identified or destroyed.

C. In the Informed consent document, researchers must describe the extent, if any, to which confidentiality of records identifying the subject will be maintained.

D. If there is an inadvertent breach of confidentiality of the research data which causes harm or places subjects or others at a greater risk of harm (including physical, psychological, economic, or social harm), the LR must report this to the IRB through the Unanticipated Problems reporting process within 5 working days of the researcher becoming aware of the event.

1. If there is such a breach, investigators should contact OIT to report that a potential security breach has occurred and request immediate notification of the

OIT security staff and the Security Breach Lead Campus Authorities. Send additional information via email to security@uci.edu with a copy to security-lca@uci.edu.

2. For a data security breach that involves protected health information under HIPAA, investigators should also contact the Hospital Compliance Office at 714-456-3674.

E. LRs wanting to create, use, or disclose PHI as part of the research activities must indicate in the IRB Application which PHI identifiers will be accessed, created, or disclosed. The LR must also submit the informed consent documents to the IRB for review and approval prior to consenting participants.

F. For studies requesting a waiver of authorization to use or disclose PHI, the LR must complete the "Waiver of HIPAA Authorization for the use or Disclosure of Personal Health Information" (Appendix T) to explain why the study meets all nine of the waiver criteria and submit to the IRB for review and approval.

G. When a study meets the criteria for exemption under 45 CFR 46.101(b)(4), Investigators may access PHI for the purpose of creating a limited data set as preparatory to research.

H. LRs may be required to sign a Data Use Agreement through UCI Sponsored Projects for data received by UCI to give assurance that the information will be protected. Similarly, for data sent outside of UCI, a Data Use Agreement may be required through the Office of Research Oversight.

I. Investigators wanting, for research purposes, to obtain California state death data files containing personal identifying information must submit an application for IRB review.

J. Additional requirements when following Department of Justice (DOJ) regulations and guidance, specifically in regards to research funded by the National Institute of Justice (NIJ):

1. All projects are required to have a privacy certificate approved by the NIJ Human Subjects Protection Officer.
2. All researcher and research staff are required to sign employee confidentiality statements, which are maintained by the responsible researcher.
3. For National Institute of Justice-funded research, a copy of all data must be de-identified and sent to the National Archive of Criminal Justice Data, including copies of the informed consent document, data collection instruments, surveys or other relevant research materials.

K. Additional requirements for research conducted within the Bureau of Prisons:

1. A non-employee of the Bureau may receive records in a form not individually identifiable when advance adequate written assurance that the record will be used solely as a statistical research or reporting record is provided to the agency.
2. Except as noted in the informed consent statement to the subject, the researcher must not provide research information which identifies a subject to any person without that subject's prior written consent to release the information.
    a) For example, research information identifiable to a particular individual cannot be admitted as evidence or used for any purpose in any action, suit or other judicial, administrative, or legislative proceeding without the written consent of the individual to whom the data pertains.
3. Except for computerized data records maintained at an official Department of Justice site, records which contain non disclosable information directly traceable to a specific person may not be stored in, or introduced into, an electronic retrieval system.
4. If the researcher is conducting a study of special interest to the Office of Research and Evaluation (ORE), but the study is not a joint project involving ORE, the researcher may be asked to provide ORE with the computerized research data, not identifiable to individual subjects, accompanied by detailed documentation. These

arrangements must be negotiated prior to the beginning of the data collection phase of the project.

II. IRB Committee Responsibilities

A. The IRB Committee will consider as part of their review, whether security procedures regarding access and storage of the data are adequate.

B. The IRB Committee will also consider whether the use of personal identifiers or codes linking the data to the participant is justifiable.

C. Any unanticipated problems related to data security will be reviewed as specified in HRP Policy # 19.

D. When a Certificate of Confidentiality has been issued for a protocol, the IRB ensures that the consent form includes:
   1. A statement that notifies subjects that a Certificate is in effect; and
   2. A fair and clear explanation of the protection that the Certificate affords, including the limitations and exceptions noted below.

E. When reviewing protocols that include the use of a Certificate of Confidentiality, the IRB ensures that the consent form discloses the Certificate's limitations and exceptions to subjects.

F. Department of Energy (DOE): When Human Research is conducted or funded by the DOE, the IRB will review and approve the "Checklist for IRBs to Use in Verifying that Human Subject Research Protocols are in Compliance with DOE Requirements", as submitted by the Lead Researcher, to verify compliance with the DOE requirements for the protection of personally identifiable information.

III. IRB Privacy Board Responsibilities

A. The IRB will review all IRB applications and human subject research proposals for adequate privacy measures and to maintain the confidentiality of the research participants and their data.

B. The IRB will review all IRB applications involving HIPAA and determine whether:
   1. The Investigator should obtain authorization from the participants to access, create or disclose PHI, or
   2. The IRB may review and approve requests for a waiver of HIPAA authorization.

C. The IRB may review and approve the disclosure of a limited data set through expedited procedures.

IV. IRB Analyst or Higher Responsibilities

A. The Analyst will pre-review all new submissions to ensure that the Investigator addressed concerns regarding privacy, confidentiality provisions and data security.

B. If the research involves HIPAA, the Analyst will ensure that the LR indicated in the IRB Application the personal identifiers that will be used, created or disclosed or if a waiver of HIPAA Authorization is requested ensure that the Investigator completed Appendix T.

C. The Analyst will contact LR to request revision to informed consent document(s) that do not contain the appropriate template language.

D. The Assistant or higher will review all continuing review submissions to ensure that the LR discussed any concerns/problems regarding privacy, confidentiality and data security that occurred during the past approval period.

E. The Assistant will provide guidance to the LR as needed (e.g., recommending the above referenced data security measures or referring the LR to UCI OIT).

F. Any unanticipated problems related to data security will be handled as specified in HRP Procedure # 19.A.

G. The Analyst may prepare the study for IRB review and approval prior to receiving the

appropriate template language. However, the reviewers must be made aware that the necessary revisions have been requested and the status of the approval must be pending receipt of these changes.