University of California, San Diego
Human Research Protections Program
Institutional Review Board
Standard Operating Policies and Procedures

Section 3.6
Privacy and Confidentiality of Research Records

Policy

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.

The IRB will determine whether there is an appropriate plan to protect the confidentiality of research data that may include coding, removal of identifying information, limiting access to data, use of Certificates of Confidentiality or other effective methods. The IRB will also determine whether methods used to identify and recruit potential participants protect subject privacy and confidentiality and whether the informed consent form adequately discloses the risks to privacy and confidentiality. Physical safeguards for research data will also be reviewed by the IRB, such as maintenance of records in locked files, separation of person-identifiable demographics data from study data referenced only to a unique study ID, etc.

Access to research data should be based on a "need to know" and "minimum necessary" standard. Investigators should use and communicate person-identifiable information about research participants only when it is essential to the scientific goals of a research study. Regarding access to personal information, the IRB will consider the methods for reducing potential privacy concerns when the private information prior to approval, when the personal information: 1) is being accessed without the participant's knowledge and explicit permission, e.g., under a waiver of consent or HIPAA authorization, before consent, during recruitment and screening, under an exempt protocol; 2) ☐concerns sensitive information; 3) involves covert observation of non-public activity.

As a general policy, the criteria used by the IRB for judging the safeguards for participant confidentiality will be those of the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Although HIPAA addresses only a specifically defined set of information called Protected Health Information (PHI) derived from healthcare service events, its principles represent a best practice for all person-identifiable research data.

In the informed consent procedure, subjects are often given assurances that the confidentiality of records identifying the subjects will be maintained. Loss of confidentiality may occur however when a court orders that research files or information be submitted as evidence in a legal matter. The court decides who has access to the files and what information may be required.

Unless there is no person-identifiable information kept in research records, complete confidentiality of records identifying the subjects may be assured only to the extent that disclosure is not compelled by court order. When FDA-regulated products are being studied, the informed consent document should state that the FDA may review and copy the subject's medical records and, if necessary, obtain the identity of the subject.

IRB members and HRPP staff use the Initial Submission Checklist and Reviewer Checklist to assist them during the review. When the only or primary risk to a participant relates to his or her privacy, the IRB review places added emphasis in eliciting what private information is involved in the protocol and how it will be used. Adequate provisions to protect the privacy interests of potential participants and participants are required from the screening and recruitment phases throughout data analysis and retention. If the protocol does not include adequate provisions to protect the privacy interests of the participants, the IRBs may not approve the protocol as written.

Waiver of Authorization to Use PHI for Research: HIPAA waiver

UC system-wide policy on Disclosure of PHI for Research Purposes adopted by UCSD permits the disclosure of PHI to a researcher without patient authorization under the following circumstances:

1. The IRB approved and certified a Waiver of Authorization; or
2. The IRB approved the protocol using a limited data set and with a data use agreement between the researcher and UCSD; or
3. The IRB approved the protocol using de-identified data; or
4. The research involves PHI of decedents; or
5. For the purpose allowed under law, such as notification of adverse events

To use or disclose PHI with an IRB-approved Waiver of Individual Authorization for Research Use of PHI, appropriate UCSD authorities must receive from the researcher requesting the disclosure of PHI, the IRB Letter of Approval that certifies all of the following:

1. Identification of the IRB and the date on which the Waiver of Authorization was approved;
2. A brief description of the PHI for which use or access has been determined to be necessary;
3. A statement that the Waiver of Authorization has been reviewed and approved by the IRB;
4. The signature of the chair or other member as designated by the IRB chair who certifies the Waiver of Authorization; and
5. A statement that the IRB has determined that the Waiver of Authorization satisfies the three waiver criteria in the privacy rule.
    a) Use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based on the presence of the following elements:
        i. An adequate plan to protect the identifiers from improper use and disclosure;
        ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research;

iii. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity;

b) The research could not practicably be conducted without the waiver; and
c) The research could not practicably be conducted without access to and use of PHI.

According to UC policy (Policy Implementation 9-11), UCSD healthcare providers may discuss with a patient the possibility of enrolling in a research protocol if the researcher is a covered health care provider who seeks an IRB Waiver of Authorization to obtain the individual's contact information. The IRB can waive authorization for this purpose, even if the research protocol requires the individual's Authorization to participate

Certificates of Confidentiality

Persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals. (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)).

A Certificate of Confidentiality is granted when the research is of a sensitive nature where the protection is judged necessary to achieve the research objectives. Research can be considered sensitive if it involves the collection of information in any of the following categories:

1. Information relating to sexual attitudes, preferences, or practices;
2. Information relating to the use of alcohol, drugs, or other addictive products.
3. Information pertaining to illegal conduct;
4. Information that if released could reasonably be damaging to an individuals' financial standing, employability, or reputation within the community;
5. Information that would normally be recorded in a patient's medical record and the disclosure of which could reasonably lead to social stigmatization or discrimination;
6. Information pertaining to an individual's psychological well-being or mental health.

Data De-identification

HIPAA contains in Section 164.514 a "safe harbor" provision that states information may be considered "de-identified" (i.e., anonymous) if it does not contain any of the following elements:

1. Names.
2. 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 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. Telephone 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)
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

The Privacy Rule requires in addition that a researcher "does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information." In other words, even if the 18 elements are removed, if a researcher knows there is a way using the remaining information to re-identify an individual uniquely, then the information is not considered de-identified.

As a policy, the IRB will use HIPAA criteria for de-identification of research data.

Procedures

1. IRB members will review recruitment and data management plans for research projects for compliance with confidentiality protections.
2. Principal Investigators will obtain a Certificate of Confidentiality, as appropriate.

Applicable Regulations

Privacy Rule of the Health Insurance Portability and Accountability Act of 1996, section 164.514
http://aspe.hhs.gov/admnsimp/bannerps.htm
http://privacyruleandresearch.nih.gov/pdf/clin_research.pdf
http://privacyruleandresearch.nih.gov/irbandprivacyrule.asp

Links

Website for Certification Information: http://grants1.nih.gov/grants/policy/coc/index.htm