Chapter 11:

Privacy, Confidentiality and HIPAA

Chapter Contents

Chapter 11
Privacy, Confidentiality and HIPAA

This chapter describes the importance of privacy and confidentiality protections as required by 45 CFR 46.111, Food and Drug Administration (FDA) regulations 21 CFR 56.111, the Health Insurance Portability and Accountability Act (HIPAA, also known as the Privacy Rule), and state and local laws. The IRBs review each study to ensure that privacy of subjects and confidentiality of data are adequately addressed.

11.1 Privacy and Confidentiality

Privacy is about people. It refers to research participants' willingness to allow access to themselves and their information. Consideration of privacy includes the time and setting where private information is given, the nature of the information given, and who receives and uses the information.

Confidentiality is about data. It refers to the handling of information that a person has disclosed in a relationship of trust, with the expectation that it will not be divulged to others without permission.

IRBs must consider the protection of privacy and confidentiality as part of their ethical and regulatory duty to protect the rights and welfare of human subjects. Maintaining privacy and confidentiality helps to protect subjects from potential harms that could occur with a breach of confidentiality, such as psychological distress, loss of insurance, loss of employment, or damage to social standing. Often, particularly in behavioral research, the main risk to subjects is the possibility of a breach of privacy or confidentiality. The IRB must consider privacy and confidentiality for the entire duration of the study. The IRB must also consider confidentiality of research data after the study is finished.

Investigators are required to maintain and protect the privacy and confidentiality of all personally identifiable information, except as required by law or released with the written permission of the subject. Subjects, including children, have the right to be protected against invasion of their privacy, to expect that their personal dignity will be maintained, and to be assured that the confidentiality of their information will be maintained. The more sensitive the data, the greater the care investigators must take in obtaining, handling, and storing data.

During the consent process, investigators must explain what information will be collected, how it will be used, who will have access to it, and what will happen to it after the study ends. When applicable, investigators should explain any special precautions they will take to ensure confidentiality of sensitive information. This will allow subjects to understand how their information will be used and decide if potential confidentiality risks are acceptable to them.

Types of Identifiable Information

Information through which subjects may be identified include names, student identification numbers, hospital ID numbers, social security numbers, driver's license numbers, home addresses, photographs, videotapes, and the like. Individuals also may be identified by description, for example, as the personnel manager in a particular company, the sixth-grade teacher in a certain school, or the pediatric nurse at a local hospital. If information or data to be collected may be traced back to individual subjects, safeguards (described below) should be provided to ensure confidentiality.

Guidelines for Protecting Confidentiality

- Limit recording of personal information to that which is absolutely essential to the research
- Store personally identifiable data securely and limit access to the Principal Investigator (PI) and authorized staff
- Code data as early in the research process as possible, and plan for the ultimate disposition of the code linking the data to individual subjects
- Apply for federal Certificates of Confidentiality in all situations for which certificates are reasonable and available. If a Certificate of Confidentiality is requested for a study, the consent must include specific language. See the IRB Informed Consent Template and Instructions. For more information about Certificates of Confidentiality, refer to: https://humansubjects.nih.gov/coc/index
- Do not disclose personally identifiable data to anyone other than the research staff without the written consent of the subjects or their legal representative. (Exceptions may be made in case of emergency need for intervention or as required by regulatory agencies).

Investigators must describe their plans for protecting privacy and confidentiality in the iStar application. The IRB evaluates the investigator's plans, including:

- The settings in which potential participants will be approached and research procedures will be performed
- The settings in which data will be recorded, reviewed, and stored
- The method for recording data and labeling samples (identifiable, coded, or anonymous)
- The amount and type of data collected (to ensure that only the minimum amount necessary is collected)
- The study staff who have access to data
- Security measures in place to prevent inappropriate access to and disclosure of data
- Release of data or samples to third parties
- Destruction or de-identification of data at the end of the study

The IRB must decide on a study-by-study basis whether there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. The IRB decision is based on the sensitivity of the information obtained in the research and the protections promised to participants.

The IRB Directors are authorized to sign Certificates of Confidentiality.

Provost Signature Authorization 7-25-2016

11.2 Limits to Privacy and Confidentiality

Depending on the subject matter of the research, there may be limits to the investigator's promise of confidentiality to the subject. An example would be if a subject reveals information about possible child or elder abuse or if the investigator and/or the research

staff discover the possibility of abuse. (See Section 13.13 – Mandatory Reporting for more information.) The informed consent form must explain any limits to confidentiality.

Mandated Reporting of Abuse

California law requires reporting of abuse or neglect of the elderly, dependent adults, and children to law enforcement and/or protective services agencies. California law also requires reporting of some communicable diseases to public health agencies. California law defines who is a mandated reporter and what agencies receive reports in each of these situations. Mandated reporting limits the confidentiality that can be promised to research participants. As a researcher, mandated reporters who observe or suspect child/elder abusive or neglect must report the incident. Student researchers although not mandated reporters, must inform their faculty advisor of their concern. Additional information is found in Section 13.13 – Mandatory Reporting.

Participants must be informed if the investigator is a mandated reporter. The informed consent form should disclose what types of information must be reported to outside agencies by the research staff.

Mandated Reporting of Positive Results of Communicable Disease Testing

California law requires health care providers to report certain communicable diseases to local health authorities. For research that includes testing for HIV infection, hepatitis, tuberculosis, sexually transmitted diseases, and other communicable diseases, participants must be told that the investigator is a mandated reporter. The informed consent form should disclose what positive test results will be reported to public health agencies (California Code of Regulations Title 17, Section 2500).

Sponsor Monitoring of Research Records

In signing the consent and HIPAA form, subjects authorize monitors and auditors from funding agencies, sponsors, and regulatory agencies to access participants' study files to verify study-related data. Investigators must ensure that only the data described in the protocol and the access agreed to by participants in the informed consent and HIPAA authorization forms is available to external monitors. Research personnel often keep "shadow" research files that contain copies of source documentation for the purpose of

protecting a subject's entire record accessible to third parties. Investigators must exercise caution to confirm that the privacy or confidentiality promised in the iStar application/informed consent are met regardless of whether records are kept in electronic or paper systems.

11.3 State Laws Addressing Privacy and Confidentiality

IRBs must consider state laws concerning privacy and confidentiality when reviewing research. Federal regulations require the IRB to evaluate the acceptability of proposed research in terms of applicable law, which includes state law. Federal regulations do not affect local and state laws that apply to protection of human research subjects or that require greater protections for subjects than federal regulations. Therefore, investigators must comply with state laws regarding privacy and confidentiality.

Research Related to HIV or AIDS

The California Health and Safety Code (Section 121075-121125) provides additional protections for confidential research records in studies relating to HIV or AIDS. "Confidential research records" includes any data in a personally identifying form (such as name, social security number, address, employer or other information that could, directly or indirectly, lead to the identification of the individual research subject) developed or acquired by any person in the course of conducting research relating to AIDS.

Confidential research records developed or acquired by any person in the course of conducting research, or a research study relating to AIDS, shall be confidential and shall not be disclosed by any person in possession of the research record, nor shall these records be discoverable, nor shall any person produce any confidential research record except in the following situations:

- Confidential research records may be disclosed in accordance with the prior written consent of the research subject to whom the confidential research records relate, but only to the extent, under the circumstances, to the persons and for the purposes the written consent authorizes. Any disclosure made pursuant to such prior written consent shall contain the following statement:

This information has been disclosed to you from a confidential research record the confidentiality of which is protected by state law and any further disclosure of it without specific prior written consent of the person to whom it pertains is prohibited. Violation of these confidentiality guarantees may subject you to civil or criminal liabilities.

- Confidential research records may be disclosed without prior written consent of the research subject to whom the confidential research records relate in the following circumstances:
    - To medical personnel to the extent it is necessary to meet a bona fide medical emergency of a research subject, and
    - To the California Department of Health Services for the conduct of a special investigation of the sources of morbidity and mortality and the effects of localities, employments, conditions and circumstances on the public health and for other duties as may be required in procuring information for state and federal agencies regarding the effects of those conditions on the public health

The content of any confidential research record shall be disclosed to the research subject, the legal representative of the research subject if the research subject is a minor, or the personal representative of a deceased research subject to whom the record pertains within 30 days after a written request is made for such records by the research subject or the legal representative.

Hereditary Disorders

The California Health and Safety Code (Section 124980) addresses confidentiality related to hereditary disorders such as sickle cell anemia, cystic fibrosis, and hemophilia.

All testing results and personal information obtained from any individual related to hereditary disorders, or from specimens from any individual related to hereditary disorders, shall be held confidential and be considered a confidential medical record except for information that the individual, parent, or guardian consents to be released, provided that the individual is first fully informed of the scope of the information requested to be released, of all of the risks, benefits, and purposes for the release, and of the identity of those to whom the information will be released or made available.

Prior consent for the release of such information is not required in the following situations:

- Data compiled without reference to the identity of any individual

- Data compiled for research purposes, so long as the research has been reviewed and approved by an IRB, who must certify its approval of the research to the custodian of the information and further must certify that in its judgment the information is of such potentially substantial public health value that modification of the requirement for legally effective prior informed consent of the individual is ethically justifiable.

NOTE: USC legal opinion interprets this statute to indicate that as long as the IRB certifies that the research is approved and that the information is of a potentially substantial public health benefit, prior consent by the subject need not be obtained in order to obtain the records from the custodian. There is some concern, however, that this may conflict with the HIPAA Privacy Rules, which would require authorization by the subject for the release of his or her medical records, whether related to a hereditary disorder or not. For research where these issues arise, the IRB and/or the Office of Compliance will interpret on a case-by-case basis.

11.4 Certificate of Confidentiality

Certificates of Confidentiality (COCs) are documents issued by the National Institutes of Health (NIH) and other federal agencies (such as DOJ, FDA, CDC) to protect against forced disclosure of identifiable research information. They allow investigators 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. COCs may be granted for studies collecting sensitive information that, if disclosed, could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. NIH will issue a COC for a study that fits the NIH mission regardless if the study has federal funding or not.

Examples of sensitive information that may require a COC include:

- Genetic susceptibility or family pedigree

- Mental illness
- High risk sexual attitudes, preferences, and practices
- Substance abuse or other illegal behaviors
- Participation in exposure effects studies that later become litigious, such as breast implants or environmental or occupational exposures

By protecting investigators and Institutions from being compelled to disclose information that would identify research participants, COCs help the investigator achieve research objectives and promote participation in studies by assuring confidentiality and privacy to participants.

The certificate states the date it becomes effective and the date it expires. A COC protects all information identifiable to any individual research participant during the time certificate is in effect. If the research extends beyond the expiration date, an extension of coverage must be requested. However, **the protection afforded by the certificate is permanent**. All personally identifiable information obtained about subjects in the project while the certificate is in effect is protected in perpetuity.

While certificates protect against **involuntary** disclosure, research subjects might voluntarily disclose their own information or authorize (in writing) the investigator to release information to others. In such cases, researchers may not use the certificate to refuse disclosure. Researchers must still comply with mandatory state and local reporting of child or elder abuse, reportable communicable diseases, or a subject's threatened violence to self or others. Additionally, the certificate does not prevent audits of the study by federal agencies such as the Food and Drug Administration (FDA) or the Office for Human Research Protections (OHRP).

The informed consent form must explain that a COC has been obtained for the study. The consent form should explain the protections it affords as well as the limitations of protection. The IRB template informed consent forms contain language that should appear when a COC is obtained.

The IRB understands there is a slight risk that data may be subpoenaed before the certificate is received and would not be protected by the certificate. In these cases, the USC IRB will decide if the risk outweighs the benefit of proceeding with participant recruitment and data collection before the certificate was granted. Data collected before

the certificate is granted are protected by the certificate once it is granted so the risk pertains only to the period of time between data collection and receipt of the certificate

How to Obtain a Certificate of Confidentiality

Investigators may choose to apply for a COC, or the IRB may require that an investigator obtain one. The following steps are required to request a COC:

- Investigator indicates in the IRB application that a COC will be requested for the study

- Investigator completes a COC application and drafts and signs a cover letter to be additionally signed by the designee.

Contact the IRB to obtain Institutional Official (IO))/IO designee signature.

- Investigator submits the application to NIH (or other agency) according to the agency's application procedures

IRB Study Approval***** Letter (may be included in IRB memo – item 1)

***IRB approval may be granted even though receipt of a COC is pending as long as the consent form(s) indicate the Principal Investigator has applied for a Certificate of Confidentiality from an HHS agency. Once received the PI must upload the certificate of confidentiality into iStar and submit an amendment to update the consent informing participants the data is covered under a COC.**

Helpful Links

- DHHS Certificate of Confidentiality Kiosk: http://grants.nih.gov/grants/policy/coc/index.htm

- DHHS Frequently Asked Questions on Certificates of Confidentiality: http://grants.nih.gov/grants/policy/coc/faqs.htm

- DHHS Certificate of Confidentiality Contacts: http://grants.nih.gov/grants/policy/coc/contacts.htm

- OPRS Essential Elements for a Certificate of Confidentiality: http://oprs.usc.edu/review/confident/

- Provost Signature Authorization 7/25/2016

11.5 Health Insurance Portability and Accountability Act (HIPAA)

The federal HIPAA Privacy Rule went into effect April 14, 2003. The law generally prohibits health care entities such as health care providers, hospitals, nursing facilities, and clinics from using or disclosing protected health information without written authorization from the individual (HIPAA authorization). The Privacy Rule is in Title 45 of the Code of Federal Regulations, in Part 160 and in Subparts A and E of Part 164. More information about the Privacy Rule can be found at the Health Information Privacy site of the Office for Civil Rights (OCR) at: http://www.hhs.gov/ocr/hipaa.

Protected Health Information (PHI)

Protected health information (PHI) is any identifiable health information relating to the individual's past, present, or future physical or mental health condition, including payment for health care. When health information is individually identifiable and held by a "covered entity" it is likely to be PHI. A covered entity is a healthcare provider, healthcare clearinghouse, or health plan that transmits health information electronically. The HIPAA rule governs the use of individually-identifiable health information when it is PHI.

HIPAA and Research

HIPAA regulations apply to research that involves the use and/or creation of protected health information (PHI). Investigators who obtain, use or create PHI must comply with HIPAA requirements during all phases of the research, from the initial identification of potential participants to the storage of data after the research ends. Investigators must limit their use and disclosure of PHI to the minimum necessary to achieve the stated goals of the research.

HIPAA regulations identify 18 elements that could be used to identify an individual

- Patient names
- Dates (except year) directly related to an individual (such as date of birth, death, hospital admission, and discharge)
- Patient postal addresses including city, state, and zip code
- Patient telephone numbers
- Patient fax numbers
- Patient e-mail addresses
- Patient social security numbers
- Patient medical record numbers
- Patient health plan ID numbers
- Account numbers
- Certificate/license numbers belonging to a patient
- Patient vehicle identifiers
- Device identifiers and/or device serial numbers specific to a particular patient
- URLs
- IP address numbers
- Biometric identifiers, including finger and voice prints, belonging to a patient
- Full face photos and other comparable images of a patient
- Any other unique patient-identifying characteristic or code

HIPAA requirements apply when investigators obtain information containing any of these identifiers from a covered entity. If investigators obtain the information directly from the participant or from sources other than a covered entity (such as a research laboratory), the information is not considered PHI and is not subject to HIPAA requirements.

Additionally, creation of PHI may also require that investigators obtain an authorization from subjects.

- If a hospital lab, CLIA-certified lab, or any other facility that is HIPAA-covered is involved in the generation of the health information, HIPAA authorization from subjects **is required**
- If health information is generated by an investigator's private laboratory or if it is done outside of the oversight of a HIPAA covered entity, HIPAA **is not required**

Investigators can obtain and use PHI for research in the following situations:

- When participants sign a written HIPAA research authorization allowing access to their PHI

  Research participants authorize use of their PHI by signing the "USC HIPAA Authorization to Use Health Information for Research" form. Participants sign the HIPAA authorization form at the same time they sign the informed consent. The two forms are separate – the HIPAA authorization form cannot be combined with the informed consent document in California.

  The HIPAA authorization form (in English and Spanish) and instructions for completing the form are available at: http://oprs.usc.edu/hsirb/hsirb-forms. This form is prepared by the USC Office of Compliance, and the form cannot be modified except as described in the instructions. If a sponsor wishes to change or add language in the form, the investigator must submit the proposed changes to the USC Office of Compliance for review and approval before the form can be used.

  State and federal laws limit the disclosure of certain PHI, even with a HIPAA authorization. Under California law, a covered entity cannot release HIV test results to a researcher unless the participant gives specific permission. Release of information about mental health treatment also requires specific permission. Federal law limits the disclosure of information about alcohol and drug treatment from medical records unless the participant gives specific permission. Participants can give specific permission for these disclosures by initialing the applicable section of the USC HIPAA authorization form.

- When the IRB grants a waiver or alteration of HIPAA authorization, allowing PHI to be used in research without written authorization from participants

  Under HIPAA regulations, IRBs and Privacy Boards have the authority to grant a partial or full waiver of the requirement for written authorization by research participants. A partial waiver of HIPAA authorization allows investigators to use PHI to identify, screen, and recruit potential participants. A full waiver of HIPAA authorization allows investigators to use PHI for all study activities without getting authorization from participants. Investigators request full or partial HIPAA waivers when they complete the iStar application. Under the Privacy Rule (45 CFR 164.512(i)(1)(i)), the IRB can grant HIPAA waivers if the following criteria are met:

  1. The use or disclosure of protected health information involves no more than minimal risk to the individuals or their privacy, based on:

     a. An adequate plan to protect identifiers from improper use and disclosure,

     b. An adequate plan to destroy the identifiers at the earliest opportunity (unless there is a health or research justification for retaining identifiers or such retention is otherwise required by law), and

     c. Adequate assurances that the protected health information will not be reused or disclosed to any other person or entity except as required by law, for authorized oversight of the research project, or for other research permitted under this policy

  2. The research could not be practicably conducted without the alteration or waiver, and

  3. The research could not be conducted without access to and use of the protected health information

If the HIPAA waiver is granted, the IRB correspondence to the investigator will document and explain the waiver.

- When the investigator obtains only de-identified health information

  HIPAA regulations allow a covered entity to use or disclose health information that has been de-identified. Health information that has been de-identified is not considered protected health information. De-identification involves removal of the 18 identifiers of the individual or the individual's relatives, employers, or household members (listed above). When investigators obtain only de-identified health information for research, HIPAA requirements do not apply; no written authorization or waiver is needed to conduct the research.

- When the investigator obtains a limited data set containing only selected identifiers

  The Privacy Rule allows investigators to obtain and use a "limited data set" for research without authorization from the participant or a waiver of authorization. In a limited data set, 2 of the 18 HIPAA identifiers remain but the other 16 identifiers are removed. Limited data sets can include the following identifiers of participants and their relatives, household members, or employers:

- Dates (date of birth, date of death, and dates of service, such as hospital admission and discharge)
- Age
- City, state, and ZIP code

Investigators must sign a Data Use Agreement to obtain and use a limited data set. The Data Use Agreement is an agreement between the covered entity holding the PHI and the investigator who receives the limited data set. The agreement explains how the data will be used and protected and identifies the obligations of the investigator using the limited data set. The USC Data Use Agreement is available at: http://policy.usc.edu/hipaa.

- When the investigator obtains information about deceased individuals

  The Privacy Rule protects identifiable health information after an individual dies. An investigator who wishes to obtain PHI of deceased people for research purposes can obtain the PHI only if certain conditions are met. The investigator must certify that the PHI is being sought solely for research on the PHI of decedents, that the PHI is necessary for the research, and that documentation of

the death of each individual will be provided if requested by the covered entity. If these conditions are met, the PHI can be used without a written authorization or waiver of authorization. Investigators must complete the form "Researcher Request for Decedents' Protected Health Information" to obtain the PHI.

NOTE: HIPAA regulations have a "Preparatory to Research" provision that permits researchers to obtain and use PHI to prepare a research proposal. Under this provision, researchers are not allowed to remove PHI from the covered entity. Because Keck Hospital of USC and LAC+USC Medical Center are different covered entities, the preparatory to research provision is not practical for a study conducted at both sites. Investigators should request a partial waiver of HIPAA authorization for recruitment and screening.

External Monitor Access to Protected Health Information

In signing the consent and HIPAA form, subjects authorize monitors and auditors from funding agencies, sponsors, and regulatory agencies to access participants' study files to verify study related data. Investigators must ensure that only the data described in the protocol and the access agreed to by participants in the informed consent and HIPAA authorization forms is available to external monitors. Research personnel often keep "shadow" research files that contain copies of source documentation for the purpose of protecting a subject's entire record accessible to third parties. Investigators must exercise caution to confirm that the privacy or confidentiality promised in the iStar application/informed consent are met regardless of whether records are kept in electronic or paper systems.

Role of the USC IRBs Related to HIPAA

The USC IRB acts as the Privacy Board for Keck Medicine of USC and LAC+USC Medical Center. In this capacity, the IRB will consider and make determinations about partial or full waivers of HIPAA authorization. The IRB reviews the HIPAA sections of the iStar application and advises investigators about HIPAA applicability and the need for written authorization. However, the Privacy Officer in the USC Office of Compliance is responsible for the content of HIPAA authorization forms. The USC Office of Compliance is also responsible for HIPAA training and oversight of HIPAA compliance at USC.

For more detailed information regarding HIPAA policies, forms, procedures, and training, please go to the Office of Compliance website: http://ooc.usc.edu/health-

information. HIPAA authorization forms for non-research activities such as fundraising, marketing, and public relations are also available at this website.