In this chapter:

11.0 Privacy and Confidentiality
   -Introduction
   -Definitions

11.1 Protecting the Privacy of Participants

11.2 Protecting the Confidentiality of Participant Information
   -Anonymity
   -Limits
   -Confidentiality Requirements for approval
   -Certificates of Confidentiality (CoC)
   -Continuing Confidentiality

11.3 HIPAA - Health Insurance Portability and Accountability Act Regulations
   -HIPAA Coordination
   -HIPAA Data Sequestration, Determinations and Processes

11.4 Confidentiality Breach - Unauthorized Release of Information
   -HIPAA Violations

Introduction

Investigators are required to maintain and protect the privacy and confidentiality of all personally identifiable information of all human subjects participating in research, except as required by law or released with the written permission of the subject. Those who conduct research under the direction of the University of Louisville must develop a plan for each protocol submitted to protect the privacy and confidentiality of subjects. Subjects have the right to be protected against invasion of their privacy, to expect that their personal dignity will be maintained, and that the confidentiality of private information will be preserved. The more sensitive the research, the greater the care is required in obtaining, handling, and storing the data. The conditions for maintaining confidentiality of the subjects and the research records are required for the life of the data. The University of Louisville IRBs serve as the Privacy Board for the institution, and in order to approve research, the IRB must be satisfied that, “when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of the data” [45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)].

Definitions

Privacy means, in the context of a research protocol, respecting an individual’s right to be free from unauthorized or unreasonable intrusion, including control over the extent, timing and circumstances of obtaining personal information from or about them. For example, individuals may not want to be seen entering a place that might stigmatize them, such as a clearly-identified pregnancy counseling center.

Confidentiality means respecting a potential or current participant’s right to be free from unauthorized release of information that the individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others without permission in ways that are inconsistent with the understanding of the original disclosure. In the context of a research protocol, “confidentiality” refers to the understanding between the participant and...
investigator (e.g., as set forth in the consent and authorization documents) as to how participant information will be handled, managed, and disseminated (e.g., shared with others) as part of the research.

**Covered Entity** can be:
- A health plan
- A health care clearinghouse
- A healthcare provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA regulations

**Private information** means individually identifiable information:
- About behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place
- Which has been provided for specific purposes by an individual and which the individual can reasonable expect will not be made public (for example, and medical record).

**Sensitive Information** is private information relating, but not limited to:
- Sexual attitudes, preferences or practices
- Use or treatment for alcohol, drugs or other addictive products
- Illegal conduct
- Information which if released could reasonably cause stigmatization or discrimination, or result in damage to areas such as financial well-being, employability, or reputation.
- Certain health information, including psychological or mental health

**Protected Health Information (PHI)** is individually identifiable health information that is:
- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Protected health information excludes individually identifiable health information:
- In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
- In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
- In employment records held by a covered entity in its role as employer; and
- Regarding a person who has been deceased for more than 50 years.

**Hybrid Covered Entity** is an entity in which some, but not all, portions of the institution must comply with HIPAA regulations

### 11.1 Protecting the Privacy of Participants

<table>
<thead>
<tr>
<th>AAHRPP Std./ Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>II.3.D</td>
<td>The University of Louisville IRB has and follows written policies and procedures to evaluate the proposed arrangements for protecting the privacy interests of research participants, when appropriate, during their involvement in the research.</td>
</tr>
</tbody>
</table>

Researchers have a duty to respect the privacy of prospective subjects. That is, the researcher allows the research subject to determine when, how, and to what extent information about him or her is communicated to others. Researchers usually protect an individual’s right to privacy by obtaining free and informed consent before collecting
personal information about him or her. The act of contacting potential subjects to seek free and informed consent to access private information may constitute a breach of privacy if the investigator does not have access to such individuals in the course of his or her usual professional activities.

The PI must describe provisions he or she will take in order to protect the privacy of the research subjects during each phase of the study. The IRB may ask for additional details regarding plans to protect subject privacy. If the planned provisions are not adequate, the IRB may not approve the study.

The PI must ensure conditions in which research procedures are performed, or research information is collected, occur in a manner which prevents their sensitive data inadvertently being viewed or overheard. In addition, the PI must also ensure the data collected is the minimum necessary to perform the research.

### 11.2 Protecting the Confidentiality of Participant Information

<table>
<thead>
<tr>
<th>AAHRPP Std./Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>II.3.E</td>
<td>The IRB has and follows written policies and procedures to evaluate proposed arrangements for maintaining the confidentiality of identifiable data, when appropriate, preliminary to the research, during the research, and after the conclusion of the research.</td>
</tr>
<tr>
<td>III.2.C</td>
<td>Researchers and research staff follow the requirements of the research protocol or plan and adhere to University of Louisville policies and procedures and to the requirements or determinations of the IRB.</td>
</tr>
</tbody>
</table>

Researchers have a duty to respect the confidentiality of personal information collected during research. Research projects vary substantially in the sensitivity of the information involved, the possibility of identifying particular individuals, and the magnitude and probability of harms that may result from identification of research subjects. Breaches in confidentiality may also have a negative impact on family and friends or the group to which the research subject belongs.

The researcher has a duty to protect research subjects from harm through unauthorized release of identifiable personal information.

**Anonymity**

When information collected through research is disseminated, research subjects normally are anonymous, unless identification has been agreed to or requested by the research subject. Often, data are presented in aggregate form which also reduces the potential to link specific responses to individuals.

**Limits**

In some instances, research results may be disclosed to the government, government agencies, the research sponsor, the IRB or its designee, a regulatory agency, or those individuals who may be responsible for financial oversight at the institution where the research is conducted. State statutes may require reporting of child abuse, sexually transmitted diseases, intent to murder, or suicidal thoughts. Additionally, in the cases of well-known individuals, those with very rare conditions, or research that requires presentation of photographs or videotapes, it may be impossible to present the data without identifying the research subject. Research subjects need to be aware of any limitations to anonymity in these situations.

In other cases, research records may be liable to subpoena in judicial and administrative proceedings, and data may be vulnerable to search warrants. Because researchers have a duty to protect the confidentiality undertaken in the free and informed process to the extent possible within the law, it is legitimate for the researcher and the institution to argue the
issue in court. In fact, this may be the only legal option open to a researcher to protect the confidentiality of research data.

Confidentiality Requirements for approval
In order to approve the research, the IRB will determine if there are adequate provisions in the research which protect the confidentiality of participants which include the following:

- Limiting the recording of personal information to that which is absolutely essential to the research;
- Storing personally identifiable data securely and limit access to the principal investigator or authorized research assistants/associates;
- Code data as early in the research as possible, and plan for the ultimate disposition of the code linking the data to individual subjects
- Apply for Federal Certificates of Confidentiality (see below) for all situations for which certificates are reasonable and available
- Do not disclose personally identifiable information to anyone other than the research team without the written consent and authorization of the subjects or their legally authorized representatives. (Exceptions may be made in case of an emergency or as required by regulatory agencies.)

Certificates of Confidentiality (CoC)
Data collection about sensitive issues (such as illegal behavior, alcohol or drug use, or sexual practices or preferences) requires the protection of confidentiality beyond preventing accidental disclosures. Under Federal law, researchers can obtain an advance grant of confidentiality, known as a Certificate of Confidentiality that will provide protection against compulsory disclosure, such as subpoena, for research data.

The investigator should delineate in the IRB application any conditions under which confidential information might be disclosed and create an informed consent document that accurately reflects those conditions, including any voluntary disclosure by the researcher. The IRB is required to determine whether the risks to subjects are minimized, informed consent is appropriate, and privacy and confidentiality protections are adequate.

The CoCs were developed to encourage participation in research by granting certain protections to a subject divulging possible compromising information. The CoCs, however, do not exempt investigators from performing ethical research nor do they allow investigators to abdicate the responsibility to act in the public good. The IRB expects investigators to act in an ethical manner and therefore comply with state law by informing subjects in the consent form of the obligation of a researcher to obey state law. Therefore, investigators are required to include a statement in the consent form that alerts potential subjects of the legal and ethical mandate compelling researchers to report known or suspected child/elder abuse/neglect. Investigators should contact the IRB staff for more information on obtaining a CoC. Additional information may also be obtained from the NIH Certificate of Confidentiality Kiosk.

Continuing Confidentiality
Once the active research has been completed, investigators should consider taking additional precautions in maintaining confidentiality that were not feasible while the research was active, including de-identifying data, archiving data in a University approved secure long-term storage service, limiting access to the data. The University policy states that records should be kept a minimum of five (5) years after submission or publication of the final project report for which the data were collected, whichever is longer. If retention requirements specified in a funding agency's regulations are longer, the agency requirements will apply. In addition, at the discretion of the university, some data may be retained longer for use in subsequent projects. Therefore, study record retention above the minimum time requirement and final disposition is at the discretion of the principal investigator.
11.3 HIPAA - Health Insurance Portability and Accountability Act Regulations

The Common Rule is a set of standards common to Federal Agencies that fund research involving human subjects. These standards attempt to minimize the risks to which human subjects are exposed and assure continuing oversight by the IRB. The FDA regulations govern clinical trials of new drugs and medical devices. The University of Louisville of Louisville Biomedical IRB will utilize FDA guidance (21 CFR 50 & 56) when reviewing research involving FDA regulated test articles. DHHS regulations acknowledge the importance of confidentiality, but the HIPAA regulations are a separate set of regulations that protect the privacy and security of the individual protected health information (PHI), regardless of funding source. The HIPAA regulations builds upon existing Federal protections and creates equal standards of privacy and security protection for research governed by existing Federal human subject regulations and research that is not.

The HIPAA regulations govern the use and disclosure of PHI that is created or received by a covered entity that relates to the physical or mental health of an individual (living or deceased), the provision of health care, the payment for health care, and identifies the individual or reasonably may be used to identify the individual. A covered entity is an institution that transmits any health information in electronic form in connection with a transaction covered by HIPAA regulations. The University of Louisville is considered a hybrid entity, which means some but not all parts of the institution must comply with HIPAA.

HIPAA Coordination

The University of Louisville has a Privacy Office responsible for the development and the implementation of HIPAA policies and procedures and overseeing compliance with HIPAA. The University of Louisville IRBs serve as the Privacy Board(s) for the institution, and in order to approve research, the IRB must be satisfied that, “when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of the data” [45 CFR 46.111(a)(7) and 21 CFR 56.111(a)(7)].

HIPAA Data Sequestration, Determinations and Processes

When a HIPAA authorization in human subjects research is not obtained, University of Louisville Policy, “Action When a Required HIPAA Authorization in Human Subjects Research is not Obtained,” # HPR-2.01 applies.

When compliance monitoring or a self-report from an investigator reveals that HIPAA authorization has not been properly obtained, the IRB/Privacy Board may determine that the information/research record/data/samples may need to be sequestered from the active study research records. If such determination is made, the PI will lose access to the collected information/research record/data/samples and sequestration may occur. If the IRB/Privacy Board determines loss of research data, the PI will sequester and the following steps should be taken.

The IRB/Privacy Board will convey the determination to the investigator through correspondence from the electronic submission system. The investigator or key study personnel will place the information/research record/data in a separate envelope which will be sealed with tamper resistant tape. The envelope will clearly be labeled with the assigned subject ID number and identified as Sequestered Data. If your study includes specimens, you will be required to notify the IRB/Privacy Board of how they will be destroyed. If your study involves electronic data sent outside of the University of Louisville, you will be required to notify the sponsor of the IRB/Privacy Boards determination. When the study is completed, the sealed and labeled envelope will be put in storage with the other study documents.

Within 10 business days, the investigator will submit a letter to the IRB/Privacy Board (and sponsor, if applicable) that will include the following information:

- Identification of the PI for the research study;
• IRB# and Study Title;
• Assigned subject ID number;
• Date the Sequestration Took Place;
• Date the sponsor (if applicable) was notified;
• A description of the process that was followed that discusses how the research record has been sequestered (e.g. electronic data being stored on a thumb drive/CD/Spreadsheet in a sealed envelope);
• Where the sequestered information will be kept;
• What security measures will be taken to keep the sequestered information secure.

The letter must include the investigator’s printed name, signature and date of sequestration.

If applicable, the study sponsor must be notified of the IRB/Privacy Boards determination along with a copy of the letter. When the sponsor responds, a copy of the response should be kept with the sequestered information/research record/data/samples.

In certain cases, the IRB/Privacy Board may determine that the investigator can obtain retrospective HIPAA Authorization from subjects when a valid HIPAA Authorization was not initially obtained. This would allow the investigator to use the data/specimens. Those determinations and instructions for the investigator will be relayed to the investigator through the ESS.

11.4 Confidentiality Breach - Unauthorized Release of Information
The IRB requires that investigators report any possible or actual unauthorized release of information. The IRB treats such a problem as non-compliance, and follows the process set forth in Chapter 3, in order to review and respond to the situation.

HIPAA Violations
If a potential violation involves PHI, the University of Louisville also treats it as a potential violation of HIPAA policies and the HIPAA privacy and security regulations. The IRB will communicate and coordinate its review and response with that required under the applicable HIPAA policies.