

Guidance and Procedures #43:
Title: Data Security in Research
Date of Last Revision: April 8, 2009

- I. [Introduction](#)
- II. [Definitions](#)
- III. [Minimum Standards and Guidelines for Specimens or Data with Identifiers](#)
- IV. [Data Security for Banks and Repositories](#)
- V. [Breaches of Data Security](#)

I. Introduction

The protection of the personal and confidential information of UCLA's research participants is one of UCLA's highest priorities. Investigators are responsible for assuring that effective procedures are in place to protect identifiable and/or confidential information collected for research purposes and that it is minimal personally identifying information necessary for successful conduct of the research.

Investigators and research staff should be familiar with the information security policies of their department or unit and [UCLA](#) and work with their department [IT managers](#) if they have any questions or need guidance on how to best manage the data security for their research. The UCLA security policies are based on those of the University of California, state laws and federal regulations.

This document provides guidance on data security resources and the minimal standards for the collection, storage, use and transmission of identifiers associated with research data or specimens.

II. Definitions

- ***Data Encryption***

Encryption is the conversion of data into a form, through use of an algorithm, which cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood

- ***Identifiers***

There are two major categories of identifiers associated with human biological specimens/data: Protected Health Information (PHI) and Personal Identifying Information (PII). In addition, UCLA defines a set of "Sensitive Data" for which access or modification is limited by law or University Policy. Each of these categories has identifiers in common. The categories are described in Table 1.

Table 1: Protected Health Information, Personal Identifying Information and Sensitive Information

Protected Health Information (PHI):	Personal Identifying Information (PII):
<p>An individual's personal and health information that is created, received, or maintained by a health care provider or health plan and includes at least one of the 18 personal identifiers listed below in association with the health information:</p> <ul style="list-style-type: none"> - Name - Street address - All elements of dates except year - Telephone number - Fax number - Email address - URL address - IP address - Social security number - Account numbers - License numbers - Medical record number - Health plan beneficiary # - Device identifiers and their serial numbers - Vehicle identifiers and serial number - Biometric identifiers (finger and voice prints) - Full face photos and other comparable images - Any other unique identifying number, code, or characteristic <p><i>Limited Data Set</i> - a limited data set can include the following identifiers: a unique number code, or characteristic that does not include any of the above listed identifiers, Geographic data (without street address), and/or dates.</p>	<p>Information about an individual which includes any of the identifiers below:</p> <ul style="list-style-type: none"> - Name - Street address - All elements of dates except year - Telephone number - Fax number - Email address - URL address - IP address - Social security number - Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account - Driver's License numbers or California or other identification card number - Device identifiers and their serial numbers - Vehicle identifiers and serial number - Biometric identifiers (finger and voice prints) - Full face photos and other comparable images - Any other unique identifying number, code, or characteristic (e.g., student identification number)
Sensitive Data	
<p>An individual's first name (or fist initial) and last name in combination with any of the following:</p> <ul style="list-style-type: none"> - Social Security Number - Driver's License Number or California ID card number - Financial account information such as a credit card number - Medical Information 	

- **Secure Physical Location**

A secure location is a place (e.g., room or file cabinet) for storing paper files, and other removable medium, computers, or equipment. Only the investigator and authorized research staff have access either through a physical or electronic key.

- **Security Breach**

A situation in which unencrypted PHI, PII or sensitive information is reasonably believed to have been acquired by an unauthorized person. A **suspected security breach** means that this information may have been lost or stolen, accessed in an unauthorized fashion or infected by a virus or worm, but it is not yet known whether the information has been compromised to meet the level of a security breach.

III. Minimum Standards and Guidelines for the Collection, Storage, Use and Transmission of Specimens or Data with Identifiers

1. Collect only the minimum identity information needed. Describe in the protocol exactly what personally identifiable data elements will be collected.
2. Remove/destroy identifiers as soon as they are no longer needed.
3. If identifiers must be retained in the data files because of specific needs of the research study, investigators must provide a justification. If the data are electronic, the information must be encrypted during storage and decrypted only when needed for conduct of the research.
4. Physically secure identifiers
 - Identifiers should be removed from data files and must be encrypted if stored electronically. Identifiers must be stored in a physically separate and secure location from the data files and the key to the code.
 - Identifiers should not be stored on laptops, PDA's flash drives or other portable devices. If it is necessary to use portable devices for initial collection of identifiers, the data files should be encrypted and the identifiers moved to a secure system as soon as possible. Additionally, lock the portable device in a secure location when it is not in use.
 - For additional information on computer security refer to [Safe Computing](#) and the [Technology Compliance webpage](#).
5. Limit physical and electronic access to identifiers to authorized research personnel.
6. Identifiers transmitted over public networks must be encrypted.
7. Identifiers and contact information cannot be distributed outside UCLA without the specific consent of research participants and approval by the IRB.

IV. Data Security for Banks and Repositories

There are additional requirements for protecting identifiers associated with specimens and/or data that are stored for the purpose of sharing with other investigators for future research purposes. Please refer to the UCLA HRPP Guidance and Procedures [Specimen and Data Repositories](#) (also referred to as “Banks”).

V. Breaches of Data Security

Breaches or suspected breaches of data security that involve identifiers or sensitive data should be immediately reported to the [IT Coordinator](#) (see Attachment B of the link) for your department and to the IRB on the [Protocol Violations, Deviations & Incidents Reporting Form](#) posted on the [UCLA OPRS Human Research Protections website](#).