

Privacy, Confidentiality, and Data Security

Paula Bistak, RN, MS, CIP, CHRC, Executive Director
Cheryl Forst, RN, BSN, CCRP, Sr. HSP Analyst
Eanass Fahmy, BS, MS, User Support Specialist

Human Subjects Protection Program
University of Medicine and Dentistry of
New Jersey



Definitions

- ***Privacy*** can be defined in terms of having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.
- ***Confidentiality*** pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the understanding of the original disclosure without permission.
- ***Data Security*** is the protection of data against the deliberate or accidental access of unauthorized personnel.

Need to Protect Identifiable Information

1. Why
 - Ethical Responsibility
 - Regulatory requirements
2. Where (are the Risks)
 - Paper files
 - Electronic data
3. How
 - Design of the Study
 - Physical Barriers
 - Technology
 - Institutional Policies
4. What (are some findings)

WHY: Ethical Responsibility

- Respect for Persons
 - Autonomy
 - Maintain privacy
 - Keep information confidential
- Trust
 - Confidence in the researcher, institution

WHY: Federal Regulations – Criteria for IRB approval of Research

- Common Rule, 45 CFR 46.111 and
- FDA, 21 CFR 56.111
- HIPAA
 - Privacy Rule, *45 C.F.R. §164*

Common Rule and FDA

- IRB Criteria for Approval

"... the IRB shall determine that all of the following requirements are satisfied... (7) When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."

- Informed Consent

- "...in seeking informed consent, the following information shall be provided to each subject...(5) A statement describing the extents, if any, to which confidentiality of record identifying the subject will be maintained..."

HIPAA Authorization Core Elements (see Privacy Rule, 45 C.F.R. §164.508(c)(1))

- Description of PHI to be used or disclosed (identifying the information in a specific and meaningful manner).
- The name(s) or other specific identification of person(s) or class of persons authorized to make the requested use or disclosure.
- The name(s) or other specific identification of the person(s) or class of persons who may use the PHI or to whom the covered entity may make the requested disclosure.
- Description of each purpose of the requested use or disclosure. Researchers should note that this element must be research study specific, not for future unspecified research.

HIPAA Authorization Waiver Requirements

- If personally identifiable information will be collected, describe:
 - The plan in place to protect identifiers from improper use or disclosure.
 - When and how identifying information will be destroyed.

WHERE ARE the RISKS?

- Paper Files
 - Faculty/Staff leaving
 - Students
- Electronic Information
 - Faculty/Staff leaving
 - Students
 - Portability of devices

HOW: Study Design

- Recruitment Procedures
 - How are you gaining access to participants?
- Data fields
 - Are all fields necessary to answer the research question? (SSN, income, date of birth)
 - Can you provide justification?
- Collection tool
 - Coding data sheet
 - Keep key separate

Study Design (continued)

- Limit access
 - Trained personnel
- Certificates of Confidentiality
 - Issued by the National Institutes of Health (NIH) to protect identifiable research information from forced disclosure.

Study Design Caution

- Secondary Subjects

HOW: Physical Barriers

- Locked files
- Locked rooms
- Privacy Screens

HOW:

Institutional Policies/Procedures

- Limits on who can be a PI
- IRB application
- Separation requirements
- Expired study requirements

HOW: Technology

Investigators and study staff must be aware of their added responsibilities when utilizing electronic data storage or sharing.

Know Security Best Practices

- Ensure a secure physical environment
- Use password protection & encryption
- Protect against network threats

Are your computer and data at risk?

- Do you use your work computer for personal use?
- Do you download business files to your personal computer?
- Are you using an outdated Internet browser?
- Do you use browser extensions and/or plug-ins?
- Is your Smartphone/PDA password-protected?
- Can any of your passwords be found in a dictionary?
- Is your laptop's hard drive encrypted?
- Is your home wireless network security-enabled?
- Do you turn off your computer completely when not in use?

Ensure a secure physical environment

- An “attacker” can’t walk away with a desktop computer, nor can a computer be lost or misplaced.
- Is the same true for all laptops, removable media (CD’s) and external flash/hard drives that store sensitive data?



Use password protection

- Passwords are “cracked” by malicious software (as well as people).
- Choose strong passwords:
 - At least 8 characters
 - A combination of mixed case and numbers
 - Use acronyms: eg., L2c@h&@w (Learn to conserve at home and at work.)

Use encryption

For:

- Data (files/folders)
- Email

File Encryption

- Encode data (text, images, video, audio, other)
- Only those with the right "key" can view the data
- **Encryption File System (EFS)** built into Windows operating systems.
- **File Vault** for MAC OS 10.4
- Simple to use
- Nothing additional to purchase

Encryption using an external data storage device

Requirements for security

- Data must be encrypted and the device physically secured
- **Flash drives** containing PHI should meet the federal requirements of the 256-bit AES (Advanced Encryption Standard) algorithm.



Ref: Federal Information Processing Standard (FIPS) 140-2.

Email Encryption

- Purchase software (e.g. Zix Secure, Entrust, eCipher)
- Provides **automatic** secure messaging by:
 - Identifying outbound email that contains Protected Health Information (PHI)
 - Encrypting the email messages that have been identified as containing PHI

Note: Data Deletion vs. Data Shredding

- Data that is deleted is still recoverable
- Software that “shreds” computer data
 - FileShredder
 - Wipe & Delete
 - WinShredder

Protect against network threats

- Make safe email practices a habit.
 - Do not:
 - Open attachments from unknown senders
 - Reply to requests for personal information (social security #, login username & password)
 - Click on unsolicited links received in an email
- Do practice safe web-surfing
 - Update your browser as new versions are released
 - Check for website encryption and valid security certificates
 - Be aware of your computing environment

Summary

- Secure computer & removable drives.
- Use strong passwords, especially for access to sensitive accounts and data.
- Encrypt sensitive data especially on portable devices and media.
- Practice safe email and web surfing habits.

Data Audit

Is confidentiality maintained?



Location of computer
Limited access
Password Protection
Source Documentation
System Controls
Training

Limited Access

- Authorized individuals
- Named in the IRB approved protocol
- Individual account
- Individual password
- Internal security safe guards (last individual who added, deleted or made alterations to the record)

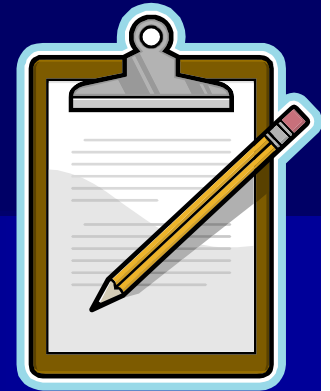


Password Protection

- No shared accounts
- Connected to the internet or intranet
- Single or double password to access data
- Multiple layers of passwords or security
- Is data stored on a flash drive
- Is the flash drive password protected
- Is the flash drive encrypted



Source Documentation



- Original observations – direct entry
- Date /Time Stamp, Electronic signature
- De-identified data links to PHI separate
- Identify source document (lab result, vital signs, depression questionnaire, H&P)
- Identify study staff, date and time of source
- Identify data entry person, date and time.

System Controls

- System should have sufficient back up
- Written back up procedures
- Encryption to protect data files
- Flash drive recommended by IST
- Procedure on maintaining data integrity, when making system design changes
- Was IRB notified of any changes?

Training

- Personnel must be listed on IRB approved protocol (fellows, students, temps, etc.)
- Staff training is conducted and recorded
- Qualified staff familiar with data entry
- Appropriately trained familiar with confidentiality
- Computer education, training and experience of study staff



Ethics of Close out

- The process of separating patients from a trial and shutting the trial down

Records and Data

- Data retention, storage and ultimate disposition
- Data and record ownership
- Destruction of “duplicate” files and documents

What does the IRB Need ?

- Location of original consent forms, official study records and documents.
- Archive information
- Final disposition of electronic data
- Whose desktop or laptop ?
- Who will maintain the data if the principal investigator should leave?

Subject Rights & Safeguards

- Secure record storage, complete with linkage capabilities
- Ability to recall a patient after separation if dictated by subsequent findings or analysis

Peace of Mind

