

Privacy, Confidentiality, and Data Security

Paula Bistak, RN, MS, CIP, Executive Director

Eanass Fahmy, MS, IT User Support Specialist

Cheryl Forst, RN, BSN, CCRP, Sr. HSP Analyst

Human Subjects Protection Program

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.

Need to Protect Identifiable Information

1. Why

- Ethical Responsibility
 - Respect for Persons
- Regulatory requirements

2. How

- Design of the Study
- Physical Barriers
- Available Technology

Ethical Responsibility

- Respect for Persons

- Autonomy

- Maintain privacy

- Keep information confidential

- Trust

- Confidence in the researcher, institution

Federal Regulations – Criteria for IRB approval of Research

Common Rule, 45 CFR 46.111 and
FDA, 21 CFR 56.111

“... 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.”

Federal Regulations (continued)

- HIPAA

- Privacy Rule, *45 C.F.R. §164*

- FDA

- 21 CFR part 11

Informed Consent Requirements

■ Common Rule and FDA

- "...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..."

■ FDA difference

- "...and notes the possibility that the Food and Drug Administration may inspect the records."

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.
- Authorization expiration date or event that relates to the individual or to the purpose of the use or disclosure (the terms "end of the research study" or "none" may be used for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the Authorization is signed by an individual's personal representative, a description of the representative's authority to act for the individual.

Authorization Required Statements (see Privacy Rule, 45 C.F.R. § 164.508(c)(2))

- The individual's right to revoke his/her Authorization in writing and either (1) the exceptions to the right to revoke and a description of how the individual may revoke Authorization or (2) reference to the corresponding section(s) of the covered entity's Notice of Privacy Practices.
- Notice of the covered entity's ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the Authorization, including research-related treatment, and, if applicable, consequences of refusing to sign the Authorization.
- The potential for the PHI to be re-disclosed by the recipient and no longer protected by the Privacy Rule. This statement does not require an analysis of risk for re-disclosure but may be a general statement that the Privacy Rule may no longer protect health information.*
_

Authorization Waiver Requirements

- Explain why/how this research involves no more than minimal risk to the subjects or their privacy.
- Explain why the waiver will not adversely affect the rights and welfare of the subjects.
- Explain why the research could not practicably be carried out without the waiver.
- 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.
 - Why the research could not be practicably conducted without access to/use of this identifiable information.

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

Physical Barriers

- Locked files
- Locked rooms
- Privacy Screens

Technology

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

Introduction to Computer & Data Security

Eanass Fahmy, BS, MS
User Support Specialist
Human Subjects Protection Program

Why?

- Hackers
- Malicious software
 - Spam, spoofs, phishes and hoaxes
 - Spyware
- Technical problems and accidents
- Theft / loss

All can compromise your computer and data.

Know Security Best Practices

1. Ensure a secure physical environment
 2. Protect against network threats
 3. Use password protection
 4. Use encryption
 5. Understand FDA 21 CFR 11
-

1. Ensure a secure physical environment

- Most office desktop computers are physically secure.
 - An “attacker” can’t walk away with the 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?



2. Protect against network threats

Definitions:

- ❑ Local computer
 - ❑ Server
 - ❑ Network share
 - ❑ Authentication
 - ❑ Core domain
-

2. Protect against network threats

- For authenticated computers:

IST and departmental IT policies are “pushed” to your computer. Eg.:

- ❑ Automatic antivirus definition & Windows updates
 - ❑ Desktop locks after 15 minutes of inactivity
 - ❑ Anti-spyware software scans
 - ❑ Blocked application lists
-

2. Protect against network threats

■ The basics (everyone):

□ Safe email practices. Eg.,

■ Don't:

- open attachments from unknown senders
- reply to requests for personal information (social security #, login username & password)
- click on unsolicited links received in email

□ Safe web-surfing

■ Don't

- load non-essential browser tools
 - click on pop-up ads (never click "No" button; close window instead)
-

3. Use password protection

- Remember: passwords are “cracked” by both people and malicious software.
 - Choose strong passwords:
 - ❑ At least 8 characters
 - ❑ A combination of mixed case and numbers
 - ❑ Easily typed
 - ❑ Something only known to the user
 - ❑ Eg: L2c@h&@w (Learn to conserve at home and at work.)
-

3. Use password protection

- Avoid using:
 - ❑ Personal “words” (favorite sports team, political figure, pet, car, etc ...)
 - ❑ Words found in any dictionary (English or otherwise)
 - Of course, do not:
 - ❑ Share passwords
 - ❑ Write them down (on desk calendar!, Post-its, etc)
-

4. Use encryption

- ❑ Files
 - ❑ Email
 - ❑ Websites
-

File Encryption

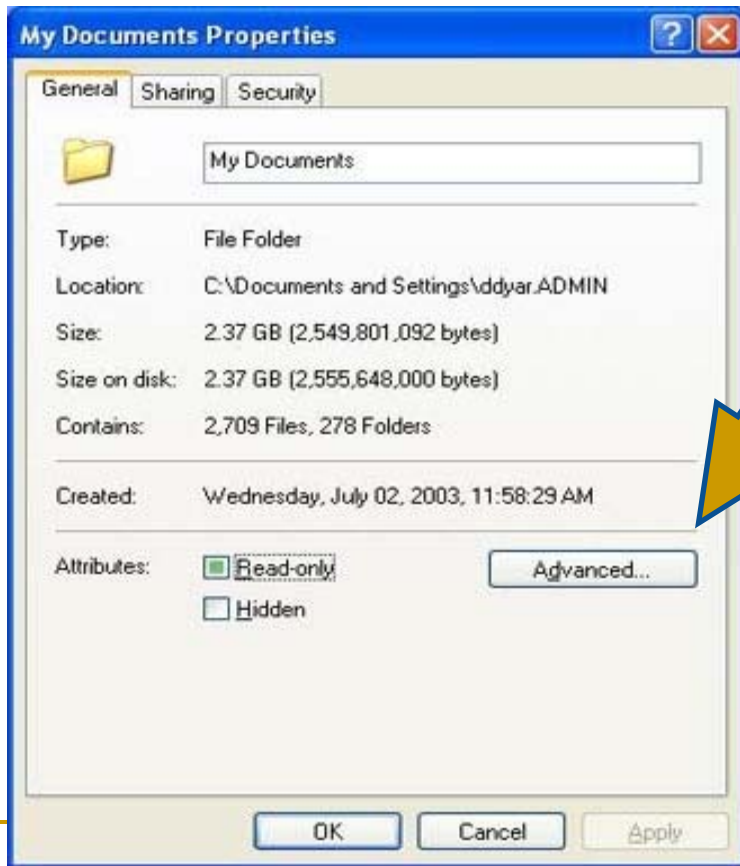
- Is the encoding of data (text, images, video, audio, other)
 - Only those with the right “key” can view the data
 - The rules that define how to encrypt & decrypt data is termed the *encryption algorithm* or *standard*.
 - Current encryption standards include:
 - Data Encryption Standard (DES)
 - Advanced Encryption Standard (AES)
-

File Encryption

- **Encryption File System (EFS)** built into Windows 2000, XP and Vista.
 - BitLocker Drive encryption for Vista Enterprise & Ultimate
 - **File Vault** for MAC OS 10.4
 - Simple to use
 - Nothing additional to purchase
-

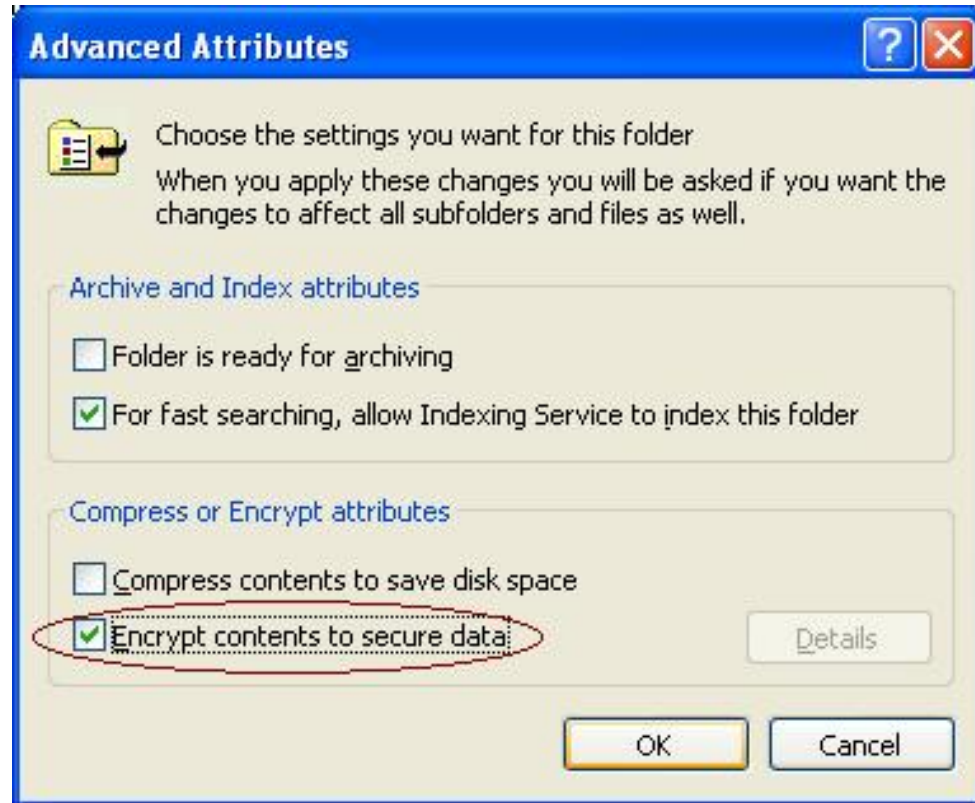
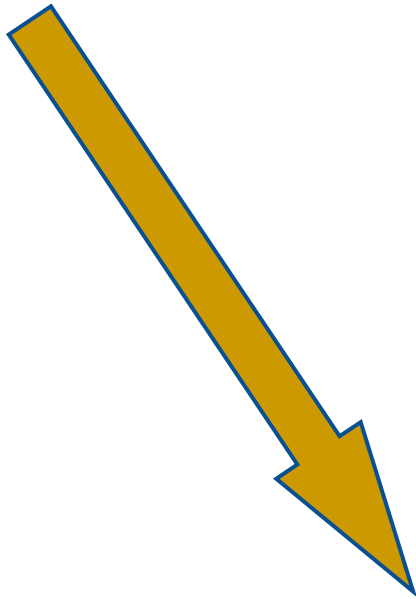
How to Encrypt a Folder? (Windows)

- Navigate to the folder to be encrypted.
- Right-click on the folder and select Properties.



Click on the Advanced button.

- Select **Encrypt contents to secure data**.



- Click OK when done.

Confirm Attribute Changes



You have chosen to make the following attribute changes:

encrypt

Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?

- Apply changes to this folder only
- Apply changes to this folder, subfolders and files

OK

Cancel

-
- **Green** file/folder name = encryption on (i.e.. an encrypt attribute set)
 - New files and folder placed inside will also have **green** names (encrypted).
 - Copying/moving an encrypted file: check file/folder color to verify status.
 - Black file/folder name = decrypted.
-

Encryption using an external data storage device

Requirements for security

- Data must be encrypted and the device physically secured.
- **Flash drives** containing sensitive PHI data should meet the federal requirements of the 256-bit AES (Advanced Encryption Standard) algorithm. This follows the "Federal Information Processing Standard 140-2(FIPS 140-2)" for ensuring the confidentiality of sensitive data and information.



Email Encryption

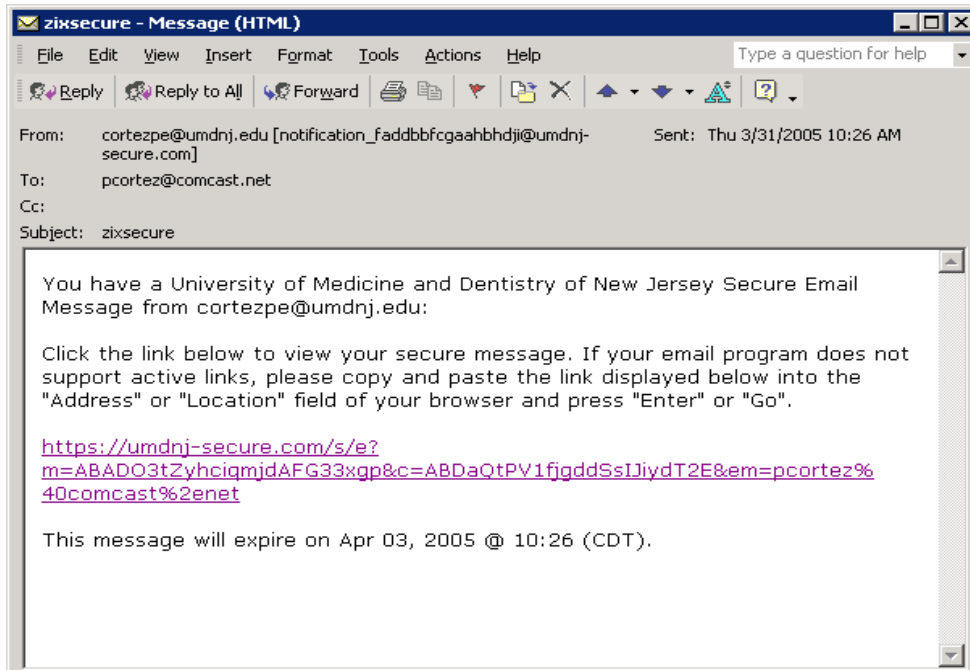
(@ UMDNJ provided by ZixCorp)

- 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
 - To **manually** encrypt an email:
 - **Type ZixSecure** into the subject line and/or the body of the e-mail.
 - <http://www2.umdnj.edu/hipaaweb/security/>
-

Sending email to a non-UMDNJ address?

- * Non-UMDNJ email addresses will require registration.

Message sent to recipient



Registration Page

The registration page features the UMDNJ logo and the text "UNIVERSITY OF MEDICINE AND DENTISTRY OF NEW JERSEY". The main heading is "Register below for your mailbox to send and receive secure messages." The form includes the following fields:

- Email Address*:
- Password*:
- Re-enter Password*:
- Password Reminder Phrase*:

Buttons for "Cancel" and "Submit Password" are located below the form. A "Password Rules" section on the right states: "Passwords must be at least six characters and must meet two of the following three conditions:"

- Contain both alphabetic and numeric characters
- Contain both uppercase and lowercase characters
- Contain at least one special character such as: ~!@#\$\$%^&

*Indicates required field

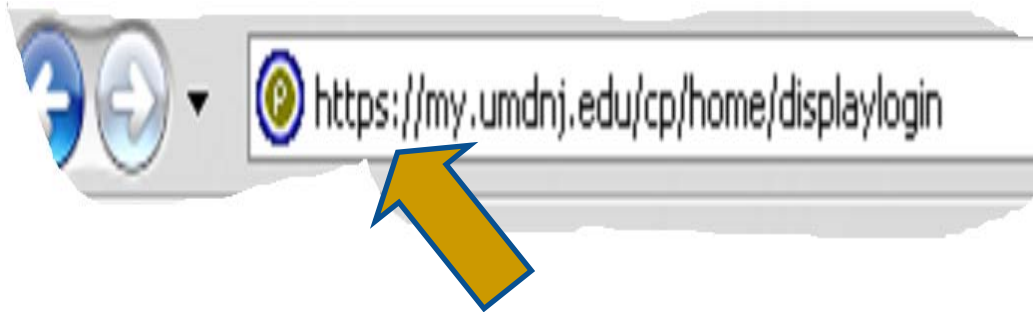
Want to receive your secure messages directly in your inbox? Learn more about [ZixMail](#).
For Customer Support, email us at support@zixcorp.com.

Secured by [zixcorp](#)

Zix Secure Messaging Instructions

Website Encryption

- Look for **HTTPS** and **SSL**



- https = Secure Hyper Text Transfer Protocol
- ssl = Secure Sockets Layer (SSL).

5. FDA 21 CFR PART 11

- ❑ Guidelines on **electronic records** and **electronic signatures** in the United States.
- ❑ Part 11 requirements:
 - implement controls, including **audits**, **validation systems**, and **documentation** for software and systems.

[FDA 21 CFR Part 11 Reference Material](#)

Audit Trail

- Who (specific user; not a generic account)
 - What (data that was added, deleted or modified)
 - When (timestamp)
-
- To be 21 CFR Part 11 compliant, must be able to produce the above upon request.
-

Summary

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

Electronic Data Audit



Is confidentiality maintained?

Location of computer

Limited access

Password Protection

Source Documentation

System Controls

Training

Limited Access

- ▶ Authorized individuals – 21CFR11.10(d)
- ▶ 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



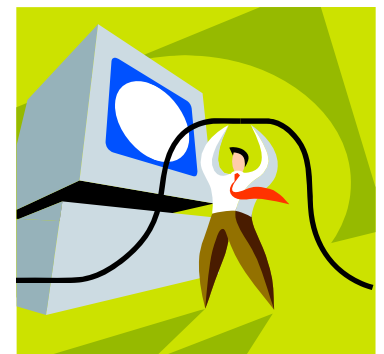
Source Documentation

- ▶ 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, ect)
- ▶ Staff training is conducted and recorded
- ▶ Qualified staff familiar with data entry
- ▶ CITI trained familiar with confidentiality
- ▶ Computer education, training and experience of study staff



Peace of mind

