Hot Topics in Research

Security of Research Data: How to Protect Research Subjects

Presented by: Shawn O’Reilly, CISA, CISM, CEH
Information Security Coordinator
Thursday, November 16

CONFIDENTIAL INFORMATION
KEEP IT SECURE!

State University of New York
Upstate Medical University

Why are you here today?

- Understand how to secure research data
- Become familiar with relevant FDA guidelines, HIPAA Security, and State Law
- Provide best practices to follow for protecting electronic information
  - Administrative procedures
  - Physical precautions
  - Technical protection

Our Mission*

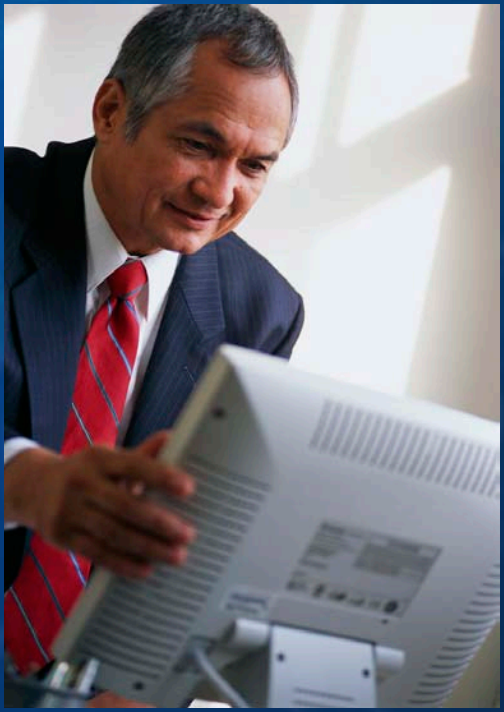
“To improve the health of the communities we serve through education, biomedical research and health care.”

- The integrated/interactive/interdependent/nature of the education, clinical service quality, and research missions so fundamental to the overall patient care mission of Upstate.
- The plan for continuous monitoring and improving the quality of care and outcomes in each area.
- Recruitment and retention of staff appropriate to provide the planned services.
- Recommendations, needs, expectations, and level of satisfaction of our internal and external customers with the programs and services.
- The quality of the environment to support the health care services and assure that planning, direction, and coordination of services is carried out.

*Hospital Plan for Provision of Patient Care Services

Importance of Security

In order to improve the health of the communities we serve, we all need to ensure our patient records and research information are properly secured.



What has happened?

- **Oct. 19, 2006 - Allina Hospitals and Clinics** - A laptop stolen from a nurse's car on October 8 contains the names and SSNs of individuals in approximately 17,000 households participating in the Allina Hospitals and Clinics obstetric home-care program since June 2005.
- **Oct. 13, 2006 - Orchard Family Practice** (Colorado doctor's patient files dumped in a parking lot)
- **June 21, 2006 - Lancaster General Hospital** - A desktop computer with personal information of hundreds of doctors was stolen from a locked office June 10. The unencrypted data included names, practice addresses, and SSNS of physicians on medical and dental staff.
- **May 3, 2006 - VA** laptop stolen from an analyst's home, contained the names, birth dates and Social Security numbers of millions of current and former service members
- **April 9, 2006 - University of Medicine and Dentistry of New Jersey** - Hackers accessed Social Security numbers, loan information, and other confidential financial information of students and alumni.
- **Feb. 1, 2006 - Blue Cross and Blue Shield of North Carolina** - Inadvertently exposed SSNs of members printed on the mailing labels of envelopes with information about a new insurance plan.
- **Jan. 24, 2006 - Univ. of WA Medical Center** - Stolen laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data.
- **January 1, 2006 - University of Pittsburgh Medical Center** – 6 stolen computers with Names, SSNs, birth dates.

http://www.privacyrights.org/

What we do not want to happen?

THE GAZETTE

“A laptop computer containing the names and social security numbers of local healthcare facility in Central New York, including their diagnosis was stolen.”

How do we prevent this?

Data

Regs

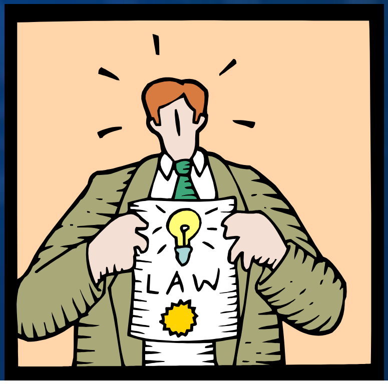
Procedures

▲ ▼ ▲

Protection and Security of Research Data

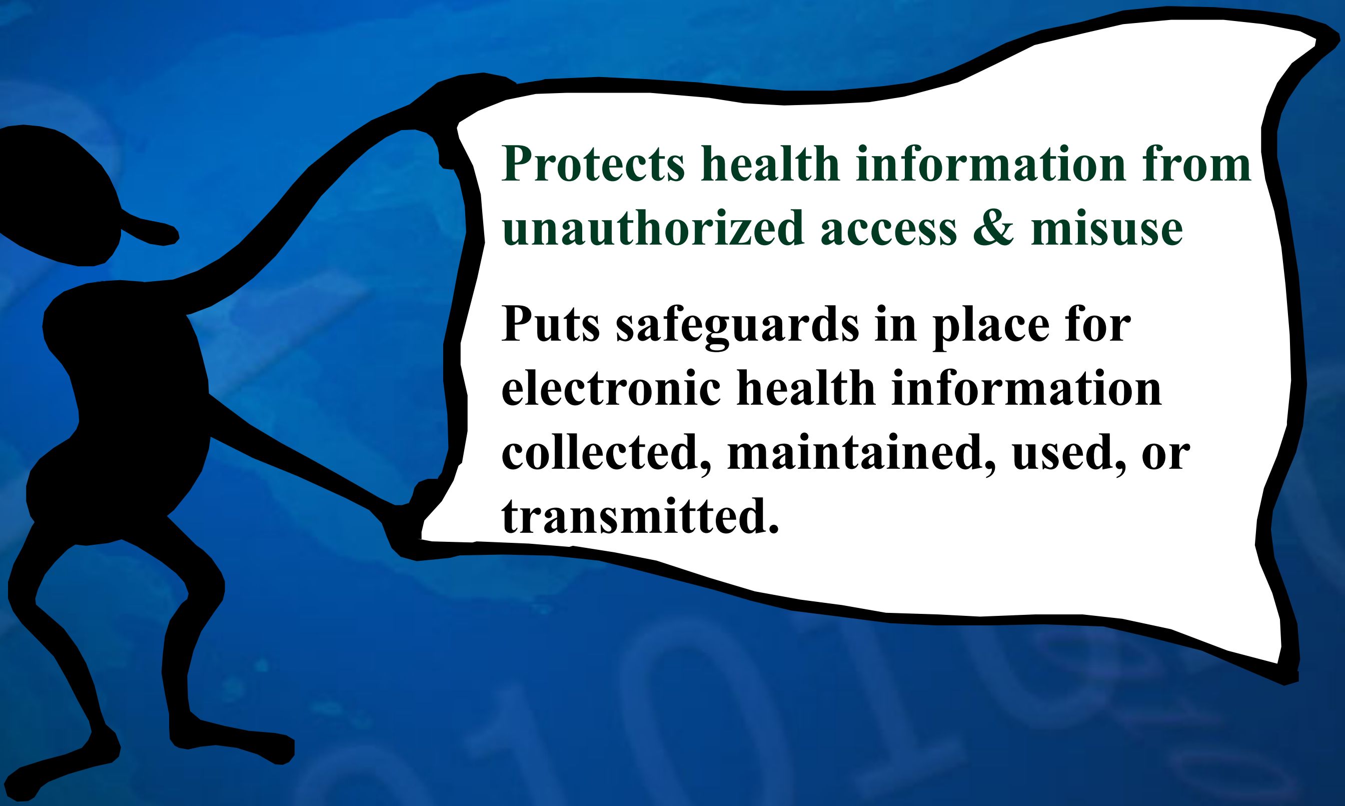
The Regs

- HIPAA Security (45 CFR Parts 160, 162, 164)
- 21 CFR Part 11 Electronic Records and Electronic Signatures
- Guidance for Industry – Computerized Systems Used in Clinical Trials
- New York State Security Breach and Notification Act



HIPAA Security (April 2005)

- National standard to protect the Confidentiality, Integrity, and Availability of electronic protected health information.

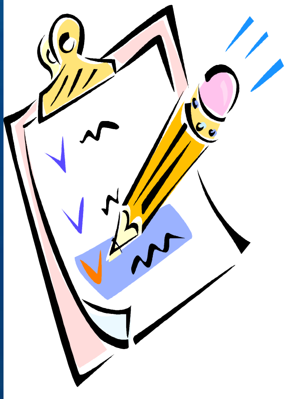


Protects health information from unauthorized access & misuse

Puts safeguards in place for electronic health information collected, maintained, used, or transmitted.

21 CFR Part 11 Electronic Records and Electronic Signatures (August 2003)

- Limit system access to authorized individuals
- Use of operational system checks, authority checks, and device checks
- Determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- Appropriate controls over systems documentation



Guidance for Industry – Computerized Systems Used in Clinical Trials

- Addresses items pertaining to computerized systems used to create, modify, maintain, archive, retrieve, or transmit clinical data.

- Focuses on the elements of data quality where computerized systems are being used to create, modify, maintain, archive, retrieve, or transmit clinical data.

New York State - Information Security Breach and Notification Act (Dec 2005)

- Law requires notification to an individual when there has been or is reasonably believed to have been a compromise of the individual’s private information.
- Private Information is personal information in combination with any one or more of the following data elements: Social security number; Driver's license number or non-driver identification card number; or Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

The Data

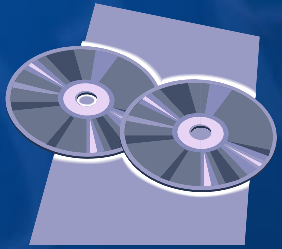
- **Questions to ponder when considering your research data needed and/or required.**
  - What data elements are required for this study?
  - Where do the data elements currently reside - electronically or in paper?
  - If electronically, what system will need to be accessed to get this information?
  - What level of access will be required to what system?
  - Will data be input into a spreadsheet or database for further analysis and review?

Protected Health Information Identifiers

- Names
- Geographic subdivisions smaller than a state (see rule for details concerning use of zip codes)
- Dates of birth, admission, discharge, and death
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical Record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers (e.g., of healthcare professionals)
- Vehicle identifiers
- Device identifiers (e.g. of pacemakers)
- URLs
- IP addresses
- Biometric identifiers
- Full face photographs
- Any other unique identifying number, characteristic, or code (e.g. blue-eyed, blond oriental who is 7 feet tall)

Electronic Protected Health Information (ePHI)

- **Electronic health and research information is any confidential patient information that is received, created, maintained, or transmitted in electronic form, including:**
  - Data entered into IMT managed information systems
  - Data entered into spreadsheets/databases
  - Electronic files sent/received through electronic mail or file transfers
  - Information stored on media/devices



Which of the following is NOT an objective to secure Electronic Protected Health Information?

A. Confidentiality	B. Reliability
C. Integrity	D. Availability

Which of the following is NOT an objective to secure Electronic Protected Health Information?

A. Confidentiality

B. Reliability

C. Integrity

D. Availability

Data Protection and the CIA

Confidentiality: → The protection of information from unauthorized access & disclosure.

- Passwords to access information

Integrity: → The protection of information from unauthorized, unanticipated, and unintentional modification.

- Research data – complete and accurate

Availability: → The assurance that information and services are accessible when required.

- Minimize system disruption

It is everyone's responsibility to protect the confidentiality, integrity, and availability of electronic patient health/research information.

So if I do NOT share my IDs and passwords to access research information I will be ensuring the CIA of this data?

NOT TRUE!!! - - -

- Have you considered what would happen to your information if your hard drive crashed?
- Are there data input checks to ensure information place in spreadsheets and databases is accurate?
- If a USB or laptop was stolen, could your data be re-created?
- Is a SSN# really required for a study?

So what can I do?

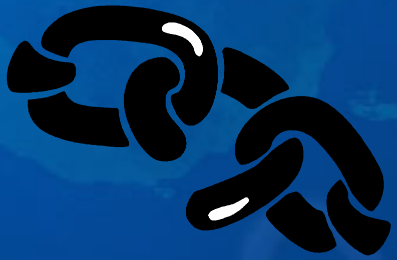
- Total security is unrealistic.
- Every environment is vulnerable to security breaches and incidents.
- The more complex the environment is, the more difficult it is to secure it effectively.

Administrative Procedures

- Written and documented procedures for how research information will be secured.
- Establish the Standard Operating Procedures (SOPs) pertinent to the use of computer systems for research.
  - User responsibility
  - Data Collection and Handling
  - Data Disasters and Backups
  - Access and Password Management
  - Remote access

User Responsibility

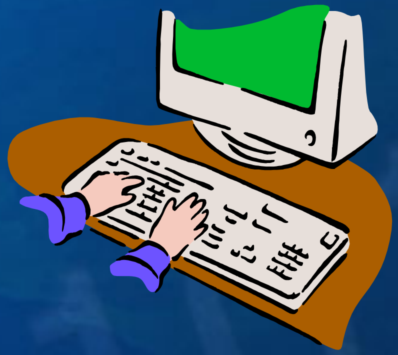
- Use good judgment when accessing information (i.e. if this were your information would you be accessing or not securing it appropriately).
- Document the procedures for how information will be generated, accessed, modified, and reported.
- The biggest threat to SUNY Upstate information is our own employees and research staff.



As the saying goes, a chain is only as strong as its weakest link.

Data Collection and Handling

- All Upstate data must be protected from errors, including those that are unauthorized and unintentional, but most importantly those mistakes made by users with authorized access to perform data entry functions.
  - Data integrity protection starts by ensuring information entered is appropriate – be sure to validate accuracy of input prior to entering information.
  - Read and review all output to confirm successful input and update of information.
  - Ensure all training requirements have been met prior to accessing and using information.



Computer Disasters

When we hear of computer disasters they usually involve an IMT system that is no longer functioning or accessible.

However, these types of disasters can occur right at your own desk or office.

Computer Backups

Protect yourself and your computer access…

- Do not leave CDs, USB Flash Drives, Disks, and other media devices out in the open – secure these devices in an office, desk, or filing cabinet.
- Ensure all backups and devices storing ePHI are properly labeled.
- Practice good housekeeping with drinks and food.
- Backup ePHI information to network drives on a regular basis. Limit the use of the local computer drive.
- Print electronic information as a secondary form of backup to protect against electronic loss.

Access Management

- Procedures should document and define who is authorized to have access to certain research information based on their responsibilities related to the research endeavor.

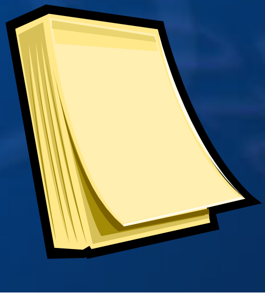
- New Process for Obtaining Access to ePHI for Research*

Password Management

- You are responsible for the management of all your passwords used to access ePHI for research. The sharing of user accounts and/or passwords is prohibited on Upstate computer systems and could result in disciplinary actions.

- Some best practices for password selection include:
  - **Select a password that cannot be easily guessed**
  - **Passwords must include a combination of number and letters (upper and lower case)**
  - **Passwords must be at least 6 characters in length**
  - **Passwords must be changed at least every 180 days**

- Use good judgment when selecting passwords.



Remote Access

If information must be accessed from outside of Upstate, the same precautions should be used to protect research information as if you were onsite.

- Document who has remote access to information, including why information cannot be gathered/accessed when onsite.*
- ll remote access should be performed through a secured and encrypted connection (i.e. VPN on an Upstate owned computer, Netstorage, RSA Key Fob if required to access patient level information).
- Use of SUNY Upstate assets are "only used for business and clinically related work."

Physical Precautions

- Physical precautions relate to the physical measures put in place to protect buildings and equipment from security threats.
- Physical precautions do not involve just public intrusions, but also natural and environmental hazards.
- Physical access could extend to your home, vacation spot, or training seminar.

Protecting Access

While protecting information encompasses use of user accounts and passwords, there are also physical components to protecting access as well:

- ❖ Always keep computer screens titled away from public areas to protect ePHI.
- ❖ If a computer has been assigned to you, make sure it is appropriately secured or turned off when you are out.
- ❖ Computers should have password-protected screen savers and keyboard locks to secure devices when they are idle for a period of time.
- ❖ Practice common sense security by making sure desks and offices/doors are locked as appropriate.
- ❖ Shred or place any confidential documents in shredding containers, including electronic media.

Computer Use and Unauthorized Software

Another source of security problems is software or hardware that is installed without approval of the IMT department.

- Music and Movie sharing software.
- Remote access software.
- Games.
- Screen savers.
- Executable files (files that end in “.exe”).
- Wireless access points.
- Routers and Hubs.

These items can cause serious breaches to the security of Upstate’s network and our ePHI.

Portable Devices and Media

If information must be taken outside of Upstate using portable media the security risks to the information significantly increase. (i.e. theft, loss, public access, destruction, environmental concerns)

- ❖ Always use passwords of devices and media as a secondary layer of protection. (PDA/Blackberries should use power on passwords).
- ❖ Ensure a copy of the data is kept onsite at Upstate.
- ❖ When available, use encryption devices and technology. (i.e. Kingston - USB encryption; PGP – laptop encryption; Entrust – File encryption)
- ❖ If devices are used in public places, proper care must be taken to avoid the risk of unauthorized access.
- ❖ Use common sense (i.e. laptop should not be left in a vehicle on a 100+ degree day)

Technical Protection

- Technical protections are technology rules and requirements for ensuring our ePHI is adequately secured and validating these protection measures are working as prescribed.   Some examples include:
  - **Access Control**
  - **Unique Identification**
  - **Automatic Logoff**
  - **Virus Protection**
  - **Encryption**
  - **Auditing/Monitoring Access**

Access Control

Regardless of the technology or information systems used (ie. CAIS or Excel spreadsheets), access controls should be appropriate for the role and function of the individual performing the research – hence the term Role Based Access.

Not everyone in your department should have or need access the same ePHI information, unless their research functions are the same.

Unique User Identification

As a society, we are all very unique and different. Everyone has their own style, clothes, food preferences, relationships, etc… The same is true for our computer accounts used to access information.

User identification is a way to identify a specific user of an information system, typically by name and/or number. This identification allows Upstate to track specific user activity when that individual is logged into a system.

Automatic Logoff

How many researchers in your department logoff the systems or applications they are in once they are finished or do systems timeout after a given period of inactivity? (ie. screen saver activates after 5 minutes)

The importance of logging off or automating the logoff process is to prevent unauthorized access to ePHI.

Viruses and Malicious Software

All Upstate computer systems have virus protection installed to protect the network from these harmful programs. The following tips will help you guard against malicious software:

- Do not open any unrecognized emails or attachments.
- If you receive any unrecognizable or suspicious email, report it immediately to the IMT Help Desk or the Information Security Official.
- Document any suspicious activity, such as unfamiliar programs appearing on your computer.
- Use the virus protection software to scan attachments and other files opened on a computer.
- Do not disable or remove the virus protection on Upstate computers.

Encryption

Encryption is a method of converting an original message of regular text into encoded text by means of an algorithm (type of procedure of formula). The importance of encryption is to scramble information so there would be a low probability of someone being able to comprehend the information.

Any transmission sent over an electronic communications network, for example email, the Internet, or a web page where ePHI information is being requested for entry must be encrypted, prior to sending.

Security Audits and Monitoring

All systems at SUNY Upstate record all access activity to patient information. Any information viewed and accessed using your account leaves a digital trail of where you go and what you do.

Auditing and monitoring access to ePHI is performed on a regular basis for compliance with regulations, therefore only access information needed to perform your research functions.

What if a breach occurs?

If there is a breach related to research information, you MUST report to the Security Official.

Some examples of security incidents include:

- Using or attempting to use another staff member's user ID and password to gain access to ePHI for research.
- Leaving a workstation signed on/unattended with access to ePHI
- Writing down or posting passwords on equipment for login purposes.
- Improper disposal of ePHI on CDs or diskettes
- Theft of equipment housing ePHI

What if a breach is NOT reported?

THE GAZETTE

"A laptop computer containing the names and social security numbers of numerous Central NY patients, including their diagnosis was stolen."

Do you want to be answering reporters questions about this and possible violations of Federal and NYS Laws?

Questions/Concerns

If you have any questions or observe/suspect that security of ePHI has been compromised, you must report to the SUNY Upstate Security Official at:

- E-mail: **oreillys@upstate.edu**
- Phone: **464-4093**

Access to Electronic PHI for Research

If not in direct patient care role:

- Study must entail recurring data needs
- Justification that it is not practicable to obtain PHI from other sources
- Access not granted for reviews preparatory to research

Process for Obtaining Access

Completion of the following:

- CAIS Access Request Form - Initiate the process
- Research Request for Access Form Completed by PI and Requestor; serves as attestation that pre-requirements have been met and conditions of access
- Data Request Form Specifies data and data elements required for the study