PROTECTING PATIENT PRIVACY and INFORMATION SECURITY
INTRODUCTION

As an agency employee, student, or volunteer of SUNY Upstate Medical University, you may see and hear confidential patient health information. We are committed to protecting the privacy of patients and the security of the health information they entrust to us. Under both State and Federal law patients have a right to the privacy and security of their health information.

A new Federal law, the Health Insurance Portability and Accountability Act Privacy Rule (HIPAA) became effective April 14th, 2003, and establishes the requirements for use and disclosure of patient information. The HIPAA Security rule became effective on April 21, 2005, and defines the information security requirements for access to patient information.

In this booklet, we will explain the HIPAA Privacy Rule, the HIPAA Security Rule, and SUNY Upstate Medical University’s privacy and security practices.
WHAT IS HIPAA?

HIPAA = The Health Insurance Portability and Accountability Act...A Federal Law Created in 1996

- Protects health information from unauthorized access & misuse
- Puts safeguards in place for health information collected, maintained, used or transmitted

It is everyone’s responsibility to secure and protect patient health information.
WHAT IS PROTECTED HEALTH INFORMATION?

All information about a patient is considered confidential, including information that:

- Is received, maintained or transmitted in ANY format

- Relates to the patient’s past, present or future medical condition, treatment or payment for care

- Identifies the patient or could be used to identify the patient
HOW CAN CONFIDENTIAL HEALTH INFORMATION BE SHARED?

To protect a patient’s privacy, confidential health information should be limited to the **minimum necessary** and only be accessible or shared with those who “**need to know**” in order to care for the patient or do their job.

- **Use:** The sharing of confidential health information **within** the organization

- **Disclosure:** The sharing of confidential health information with others **outside** the organization
PRIVACY SAFEGUARDS

• Shred all paper containing confidential health information or place in closed receptacles

• When faxing, verify the fax number before sending

• Close doors or privacy curtains and lower your voice when having discussions of confidential health information

• Do not leave medical records unattended or in open areas

• Keep confidential health information you hear or see to yourself

• Before looking at patient information ask yourself “Do I need to know this to do my job?” and if not, don’t look at anything

• Respect the privacy rights of employees who come here for care by affording their information the utmost confidentiality it deserves
SECURITY SAFEGUARDS

Some examples of security safeguards include:

- Do not use or attempt to use another staff member’s user ID and password to gain access to ePHI
- Never leave a workstation signed on/unattended with access to ePHI
- Writing down or posting passwords on equipment for login purposes is not permitted
- Properly dispose of ePHI on CDs, DVDs, or thumb drives
- Prevent theft of equipment housing ePHI
- Never disable or remove virus detection software

It is your responsibility to be aware of these safeguards and follow them in everyday practices.
WHAT DO YOU NEED ACCESS TO?

- Dependent on your position and job responsibilities

- Your supervisor will identify and approve the systems you need access to

- Contact the IMT Help Desk with any questions
PASSWORD MANAGEMENT

You are responsible for the management of all your passwords used to access ePHI. 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

Be sure your passwords meet the requirements outlined above!
WORKSTATION USE AND SECURITY

In order to access ePHI, you will need to login using a workstation. Workstation use and security are crucial to the security and access to information.

Workstation use and security practices include:

• Lock workstations when not in use, either using a password protected screen saver or logging off the workstation

• Workstations must be positioned or located in secure areas

You are responsible for securing our workstations and protecting our ePHI.
SECURITY AUDITS AND MONITORING

All systems at SUNY Upstate record all your activity. The information you view and access using your account leaves a digital trail of information – where you go and what you do.

SUNY Upstate audits and monitors access to ePHI systems on a regular basis, therefore only access information that you need to do your job.

If you have inappropriately accessed information, you have breached our security policies and practices!
THE SHARING OF SOME CONFIDENTIAL HEALTH INFORMATION REQUIRES EXTRA CAUTION!

The sharing of confidential health information related to certain treatments and services are afforded a higher level of protection under New York State Laws, for example:

- Alcohol/Substance Abuse
- Child Abuse
- Mental Health
- Genetics
- HIV-Related Information
- Oral Disclosure Requires Written Authorization

Do not share any confidential health information of this nature, unless you have checked with your immediate supervisor!
PERSONAL CONSEQUENCES FOR INAPPROPRIATE ACCESS

The penalties that can be levied against an individual for violating these rights can be severe, and include:

• **Termination** of employment at SUNY Upstate

• Charges of professional misconduct and loss of licensure by the NYS Education Department [NYS Education Law § 6530(23)]

• Criminal and civil monetary penalties imposed by the Department of Justice

• Criminal and civil monetary penalties imposed by the New York State Attorney General
INDIVIDUAL CIVIL MONETARY AND CRIMINAL PENALTIES UNDER HITECH FOR VIOLATING PATIENT PRIVACY

- Knowingly or wrongful uses or disclosures of PHI fined up to $50,000 and 1 year prison

- Offense committed under false pretenses fined up to $100,000 and 5 years prison

- Offense committed with intent to sell, transfer or use PHI for personal gain $500,000 and 10 years prison
Three employees at Tucson’s University Medical Center have been fired for violating patient privacy in connection with accessing confidential medical records in the high-profile shooting rampage that killed six people and left Congresswoman Gabrielle Giffords in critical condition, hospital officials said.

All the remaining injured patients from the shootings, including Giffords, are at UMC.

"The hospital has terminated three clinical support staff members this week for inappropriately accessing confidential electronic medical records, in accordance with UMC's zero-tolerance policy on patient privacy violations," says a statement issued by UMC officials this morning.

A contracted nurse also was terminated by the nurse's employer, officials say, and the families of the affected patients were notified.
SOCIAL NETWORKING SITES

Confidential Health Information about a patient should **never** be posted on a social networking site such as Facebook, MySpace, Twitter, etc. for personal use even if the patient may be the only person who may be able to identify him or herself based on the description.

Access to confidential patient information of SUNY Upstate is permitted so care and treatment can be provided to the patient, **not** for personal use!
WHO DO I CALL?

Each organization must have a Privacy and Security Official to ensure compliance with privacy and security policies. If you observe or suspect that the confidentiality or security of a patient’s health information has been violated, you must report it to your supervisor, or the SUNY Upstate Privacy Official or the SUNY Upstate Security Official at:

E-mail: nappac@upstate.edu (Privacy Official)
Phone: 464-6135

E-mail: oreillys@upstate.edu (Security Official)
Phone: 464-4093

Hotline: 464-6444 (for anonymous reports)

We cannot punish you for reporting suspected violations incidents, and in fact, it is considered your responsibility to make such a report!
The relationship between a patient and a healthcare provider is based on trust. The healthcare provider must trust the patient to give full and truthful information and the patient must trust the healthcare provider to respect the privacy of such information.