PROTECTING PATIENT PRIVACY and INFORMATION SECURITY
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 21st, 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

SSSHH!
WORKFORCE AS PATIENTS

• A workforce member's patient account is periodically audited to determine who has accessed his/her information

• Inappropriate access, use and disclosure of a workforce member's patient information is not tolerated and will result in serious consequences to the offender

• Workforce members seeking care at University Hospital who believe their patient information has been inappropriately accessed or shared should contact the SUNY Upstate Privacy Officer

• The protected health information of workforce members seeking care as a patient cannot be disclosed to the workforce member's co-workers or supervisor without authorization of the workforce member
SECURITY SAFEGUARDS

- Passwords selected must be strong passwords that are difficult to guess and must remain confidential.

- It is important to not disable the anti-virus and/or anti-spyware software on Upstate computer system.

- Log off or secure your computer when you walk away from it.

- Users should not transmit and/or store sensitive and/or confidential information on file sharing or text messaging applications.

- Back up your files if your mobile device is stolen to avoid losing all of the information. Make backups of any important information and store the backups in a separate location, preferably on Upstate systems.

- Be wary of downloadable 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
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!
USING AUDIO-VISUAL RECORDINGS TO CAPTURE PATIENT INFORMATION

- Use of cell phone cameras or other personal recording devices by staff to record patients is not permitted

- Patients may be recorded for marketing, education, or research purposes with their consent

- Patient recordings made for care and treatment do not require patient consent

- Recordings for the patient’s own use cannot be made by Upstate staff

Refer to University Hospital Administrative Policy P-46: Consent for Photography or Other Recordings for Marketing, Education, Research or Scientific Purposes
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!
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 affiliation 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
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, the Privacy Official or the Security Official at:

For Community or Downtown Campus

E-mail: connorj@upstate.edu (Privacy Official Community Campus)
Phone: 492-5090

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

E-mail: oreilys@upstate.edu (Security Official for Community and Downtown Campus)
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.