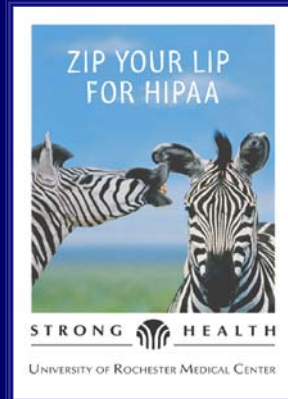




HIPAA Basic Training for Resident Physicians



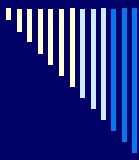
2005



HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) ensures that medical information shared with physicians, hospitals, payors and others who provide and pay for health care is protected and kept secure. HIPAA regulations:

- /// **Impose restrictions on the use and disclosure of protected health information (PHI)**
- /// **Give patients a number of rights, including greater access to their medical records**
- /// **Maintain the security of electronic PHI**



HIPAA Privacy: A Compliance Overview

All covered entities (health care plans, clearinghouses and health care providers) needed to be in compliance with HIPAA privacy since April 2003.

In response, URM/Strong Health:

- /// created policies, procedures and technical controls to ensure that PHI is kept confidential,**
- /// named Privacy Officers for each entity within URM/SH,**
- /// provided training for the workforce in these regulations, and**
- /// notifies patients in writing of their rights under HIPAA.**



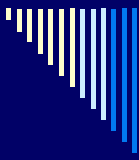
Compliance is Mandatory

Civil monetary penalties range from \$100 per violation, with the maximum penalty not to exceed \$25,000 per year for each standard violated.

Criminal penalties for knowing violations:

- Wrongful disclosure \$50,000 and/or 1 yr in prison**
- Obtaining information \$100,000 and/or prison for**
under false pretenses up to 5 yrs
- Intent to sell \$250,000 and/or up to 10 yrs**
in jail

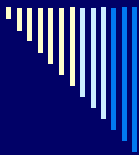
A confidentiality violation may also result in a Type 1 recommendation from JCAHO and/or a citation from the Center for Medicare/Medicaid Services (CMS).



PHI **Protected Health Information**

Is defined as any information—oral, recorded, paper or electronic, concerning:

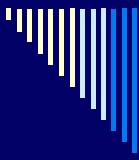
- /// **Past, present or future physical or mental health or condition of an individual**
- /// **Provision of healthcare to an individual, or**
- /// **Past, present or future payments for the provision of healthcare to an individual**



Minimum Necessary Standard

URMC/Strong Health Policies have been implemented to limit the uses and disclosures of PHI to the amount reasonably necessary to achieve the purpose for payment, health care operations or in any disclosure not authorized by the individual.

***Exception:* Minimum necessary standard does not apply to the use or disclosure of PHI for treatment of an individual.**

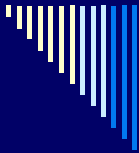


Privacy Regulations

PHI May Be Used or Disclosed in One of the Following Ways:

- 1. For treatment, payment or health care operations; or**
- 2. By patient authorization; or**
- 3. With the patient's agreement in limited situations; or**
- 4. Regardless of a patient's wishes, such as when required by law**

Exception: Patients must grant authority to disclose PHI when receiving research related care, such as a drug trial.



PHI Disclosed by Patient Authorization

Some examples where disclosure of PHI requires signed patient authorization include:

- ⚡ For marketing purposes (except regarding treatment options)**
 - ⚡ To the media**
 - ⚡ To the patient's employer, school, attorney, life insurance company, disability carrier, etc.**
 - ⚡ For research related to care (drug trials)**
-



Limited PHI That May Be Disclosed With the Patient's Agreement

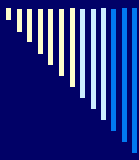
- ⚡ **If a patient has agreed to be listed in the hospital's public facility directory, his or her location and general one-word condition (satisfactory, guarded) can be released to those who ask for the patient by name.**
 - ⚡ **If a patient chooses to list a religious affiliation, a clergy member of that faith may receive a list of patients who have listed that religion. This is an exception to having to ask for the patient by name. The only information that can be provided to the clergy is the patient's name, location and one-word condition.**
 - ⚡ **If a patient identifies a family member or person as being involved in his/her care, a physician can speak with that family member or person whom the patient has identified.**
-



PHI Disclosed to Appropriate Authorities Regardless of a Patient's Wishes

Some examples of disclosures required by law:

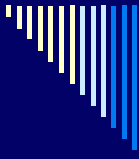
- ⚡ **Suspected child abuse**
 - ⚡ **Public health issues which are reportable**
 - ⚡ **Reporting to state mandated registries (Tumor Registry, etc.)**
 - ⚡ **Medical devices/supplies are recalled**
-



Notice of Privacy Practices

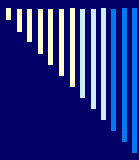
Patients must receive a copy of the Notice of Privacy Practices which outlines:

- ⚡ How their PHI may be used or disclosed;**
 - ⚡ Their right to inspect and request copies or amendments to their medical records; and**
 - ⚡ How to file a complaint with URM/Strong Health or the Secretary of Health & Human Services if they suspect violations of the Privacy Rule have occurred.**
-



Privacy Helpful Hints for Residents

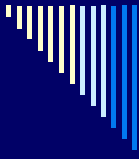
- ⚡ If there is a visitor present in an inpatient or ED treatment room and you do not know if the patient wishes to have his/her PHI disclosed in front of the visitor, it's a good idea to politely ask the visitor to step out for a few minutes while you speak with your patient. The patient may indicate that it's okay for the visitor to stay, which is fine. However, the patient may not wish the visitor to hear what's being discussed and may not want to say so directly. Of course if you know the visitor to be the patient's family member with whom you have the patient's agreement to share PHI, the family member does not have to be asked to leave. There have been several privacy complaints where a visitor has turned out to be the patient's coworker, neighbor or even family member that the patient was not comfortable sharing PHI with, resulting in complaints against physicians.**
-



Privacy Helpful Hints for Residents (cont.)

- /// You are only permitted to access those records for patients with whom you have a clinical or business reason to do so. There is an exception which permits MDs to access their own personal PHI. However, this exception does NOT extend to the MD's family members, coworkers or any other patients with whom you do not have a treatment relationship. Residents who violate this policy will be sanctioned.**

 - /// If you have a question concerning whether a use or disclosure is permitted, contact the entity's Privacy Officer.**
-



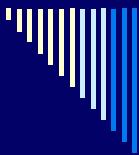
HIPAA Security Regulations

Security standards support the Privacy regulations and are specific to electronic protected health information (ePHI). HIPAA Security has a compliance date of April 2005 and covers:

- /// Confidentiality (ePHI is not made available or disclosed to unauthorized persons)**

 - /// Integrity (ePHI has not been altered or destroyed in an unauthorized manner)**

 - /// Availability (ePHI can be accessed when needed by those with authority to do so)**
-

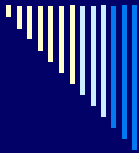


Components of HIPAA Security:

- /// **Administrative Safeguards**
 - ✓ **Designation of HIPAA Security Officials, policies, contingency plans, sanctions, password management, termination procedures, training, etc.**

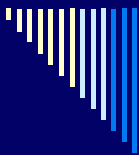
 - /// **Physical Safeguards**
 - ✓ **Workstation use and security, facility access and security, device controls, disposal, etc.**

 - /// **Technical Safeguards**
 - ✓ **Access control, unique user ID, integrity controls, auto log-off, authentication, audit, transmission safeguards, anti-virus, etc.**
-



Security Helpful Hints for Residents

- /// **Never share your password to any application containing ePHI with anyone, ever!**
 - /// **If you have a personally-owned hand-held digital device containing ePHI (PDA, laptop, etc.), you are the system administrator for the device and need to follow all policies accordingly.**
 - /// **ePHI must be kept under your control at all times, whether you are in the hospital, at an off-site location, at home, etc.**
 - /// **Remember that your access to any electronic patient record may be monitored.**
-

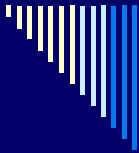


URMC/Strong Health HIPAA Officers

- /// **Strong Memorial Hospital Privacy Officer: Pat Beato (784-6154)**
- /// **Research Privacy Officer: Pete Chesterton (275-7059)**
- /// **Strong Memorial HIPAA Security Official: Chip Nimick (784-6115)**
- /// **Research HIPAA Security Official: Pete Chesterton (275-7059)**

for a complete list of URMC/SH HIPAA officers and more information on HIPAA, please go to:

<http://intranet.urmc.rochester.edu/HIPAA/>



Next Steps to Complete HIPAA Training:

- /// **HIPAA Privacy & Security Job-specific training will need to be completed in your department/program within 30 days of orientation. Read those training modules required for all workforce members, as well as the modules for those with access to PHI.**
- /// **Training modules can be found on-line at:
<http://intranet.urmc.rochester.edu/policy/HIPAA>**
- /// **Contact your program coordinator for more details and to record your training compliance.**