HIPAA Compliance
2013 Annual Mandatory Education
What is HIPAA?

Health Insurance Portability and Accountability Act – Federal Law enacted in 1996 that mandates adoption of

- Privacy protections for health information (“Privacy Rule”)
- Administrative, technical and physical safeguards to protect the security of electronic health information (“Security Rule”)

What does HIPAA mean to patients and providers?

- Sets rules and limits on how providers may use and disclose Protected Health Information (PHI)
- Establishes rights for individuals with respect to their PHI
Who must comply with HIPAA?

• HIPAA applies to “Covered Entities” and “Business Associates”
• Covered Entities include certain health care providers and health plans. Common examples include:
  – Hospitals
  – Physician practices
  – Ambulatory surgery centers
  – Imaging centers

• Business Associates include any person or entity that:
  – Assists a Covered Entity in performing, an activity or function that requires the use or disclosure of PHI, or
  – Provides legal, actuarial, accounting, management, administrative, accreditation or financial services where the provision of such services involves the use and/or disclosure of PHI from a Covered Entity

Business Associate Agreements must be executed between Covered Entities and Business Associates before PHI may be shared
Why do we need to know about HIPAA?

- As a covered entity, all Tufts Medical Center employees and members of its workforce must comply with the Privacy Rule and Security Rule.
- Tufts MC staff must use “reasonable safeguards” to protect the information against inappropriate use and disclosure and must employ the “minimum necessary” standard.
  - Derived from confidential codes/practices long practiced in medicine and nursing.
  - Personal Health Information (PHI) should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.
  - Does not apply to:
    - Disclosures to or requests by a health care provider for treatment – this is the critical exception to this rule!
    - Certain other exceptions.

Ask yourself: “What do I need to know to carry out my job duties or responsibilities?” …. If you do not need the information to carry out your professional responsibility, you should not access the information.
What is Protected Health Information (PHI)?

PHI includes:

- Name
- Address, including email address
- Telephone Number
- Social Security Number
- Medical Record Number

Examples of PHI are:

- Information about health condition
- Information about health services the patient has or is using
- Information about the patient’s benefits covered by insurance
- Demographic information
- Unique numbers that can identify the patient

• Providers may use/disclose PHI, without the patient’s authorization for:
  – Treatment
  – Payment
  – Health Care Operations*

*The term Health Care Operations has a specific legal meaning. Please contact Risk Management or the General Counsel’s Office for more information on any of the above classifications before disclosure of PHI.
• Under HIPAA, patients have the right to:
  – Inspect and copy records containing their PHI
    • All requests must go through Medical Records Department
  – Request an amendment to their records
  – Receive an accounting of disclosures of their health information upon request
  – Request confidential communications
  – Request additional privacy protections
How can PHI be disclosed?

- Email – via computer, mobile and tablet devices
- Telephone
- Paper or electronic records
- Voicemail
- Fax transmissions
- Verbal communications
- Facebook/Myspace Accounts

Tufts MC staff must provide patients with written copies of the provider’s “Notice of Privacy Practices”

- Describes how the patient’s health information may be used/disclosed by the provider, how the patient can access his/her information and other rights the patient has regarding his/her health information
  - Patient must sign an acknowledgement of receipt
  - Signed copy is placed in the patient’s chart
Disclosure of PHI to Family Members and Others

A provider may disclose to a family member/significant other or any other person identified by the patient, relevant information if:

- The patient agrees to the disclosure;
- The patient does not object when provided with an opportunity to object; or
- The provider reasonably infers from the circumstances, based upon professional judgment that the patient does not object

There are other circumstances where patient authorization is not required...

- Public Health Activities
- Reporting Abuse/Neglect/Domestic Violence
- Health oversight activities conducted by government agencies
- Disclosures to avert a serious, imminent threat to health/safety
- Product monitoring/recall
- Certain law enforcement activities

*All other uses and disclosures of PHI require the patient’s written authorization*
Categories Requiring Special Protection

• Some categories of information are considered so sensitive that additional protection is required. This means that even if the information relates to treatment, authorization from a patient may be required.

• In most cases, the following health information may not be disclosed without the patient’s written authorization:
  – HIV and Genetic testing and results
  – Records pertaining to venereal or sexually transmitted diseases
  – Sensitive information:
    • Sexual assault counseling records
    • Communications/notes between patient and social worker/psychologist/psychiatrist/psychotherapist/licensed mental health nurse
  – Drug/alcohol abuse treatment records
Information Security Standards

• HIPAA security rule standards are broken up into three categories:
  
  – Administrative Safeguards (such as policies and procedures)
  – Physical Safeguards (such as locks, doors, walls, identification badges)
  – Technical Safeguards (such as automatic log-off, passwords, encryption and decryption, user verification, and audit controls)
Why is Data Security Important?

• Increasing use of electronic transactions and electronic medical records

• Increasing number of instances of improper disclosures of medical records/information...examples include
  – Intentional hacking of medical system computer system and thousands of records accessed
  – Insurance company e-mailed highly sensitive personal health information to the wrong members
  – Institution posted psychological records of children and teenagers on a public website
  – Data loss resulting from transfer of unencrypted files on USB’s, laptops and transmitting files to a personal computers.

• Excellent clinical care depends on the integrity of the data; assurance that the data has not been tampered with, altered by unauthorized persons, or exposed to computer virus’ or malware.
Safeguards and Good Practices

- Speak softly when another patient or individual is nearby (i.e. double room)
- Speak to patient/family in private rooms, not waiting rooms
- **Protect** charts/results by keeping them in restricted areas
- Do not leave any printouts containing PHI in conference rooms, out on desks, etc.
- Make sure fax cover sheet has a confidentiality notice, and validate recipient before sending the fax
- **Shred** all papers with PHI or dispose in locked bins
- Log off computer or close out of an application when finished; do not leave a workstation that has PHI on the computer screen
- Position computer so passers-by cannot view the screen
- **Protect** your computer passwords: *Never share them!*
- All electronic devices (including laptops, thumb drives, etc.) must be password protected and, if possible, *encrypted*
- Do not transmit PHI via Internet unless the data is encrypted; if you have questions, please call the Help Desk or email *TuftsMCISInformationSecurity@tuftsmedicalcenter.org*
Email Guidelines

• Email within Tufts Medical Center network or “firewall” is secure and protected
  – May be used to communicate to providers within Tufts MC network without the patient’s consent

• Email sent outside the Tufts MC “firewall”/network is assumed not to be secure and should not contain PHI unless the patient consents in writing to the use of email for communication about his/her PHI
  – Prior to sending email outside of Tufts MC “firewall”/network, the provider must have the patient sign a consent form authorizing use of email communications
    – Forms and guidelines are found on the Tufts MC Intranet

• Encrypt emails sent outside the Tufts MC “firewall”/network by adding the words “Send Secure” or “Encrypt” to the beginning of the subject line
  • This must be done for each email sent outside the “firewall” that includes PHI
  • Guidelines are found on the Tufts MC Intranet – Information Services
Requirements of the HIPAA Breach Notification

• Organization must first determine whether there has been a “Breach”
  – Was there an impermissible acquisition, access, use or disclosure not permitted by the HIPAA Privacy Rule?
    • Examples include
      – Laptop or other portable device containing PHI is stolen …this includes all mobile devices that may contain PHI
      – Individual who is not authorized to access PHI receives or discloses PHI

• IMMEDIATELY contact the Tufts MC HIPAA Privacy or Security Officer if there is an actual or suspected unauthorized acquisition, access, use or disclosure of PHI by you or a co-worker

• Your departmental supervisor
• HIPAA Hotline – 617- 636 – 4422
• TuftsMCISInformationSecurity@tuftsmedicalcenter.org
• Tufts Medical Center Privacy Officer – Jeffrey Weinstein
• Tufts Medical Center Security Officer – Sonia E. Arista
HIPAA Breach Notification Provisions…

• If a breach has occurred, Tufts MC may be obligated to provide notice to:
  – The affected individuals (without unreasonable delay and in no event later than 60 days from the date of discovery)
  – Secretary of HHS (timing will depend on number of individuals affected by the breach)
  – Media (only required if 500 or more individuals of any one state are affected)

• There may also be notification requirements under the laws of any state where an affected individual resides

• Violations could lead to significant monetary penalties for Tufts MC.
  • “reasonable cause,” -the penalty could range from $1,000-$50,000 per violation, up to maximum of $1.5 million per year for all violations of an identical requirement.

  • “willful neglect,” and corrected within a specified time period, the penalty could range from $10,000-$50,000 per violation, up to maximum of $1.5 million per year for all violations of an identical requirement.

  • “willful neglect,” and not corrected within a specified time period, the penalty is $50,000 per violation, up to maximum of $1.5 million per year for all violations of an identical requirement.

• Criminal penalties include prison confinement – and can be imposed on the individual who wrongly obtains or discloses protected health information.
  • Range of 1-10 years depending upon offense
Reminders

• Do not disclose PHI without patient authorization. If you have questions about whether a disclosure is permitted, ask your supervisor, or call the HIPAA Hotline – 617-636 – 4422.

• If you think there has been an unauthorized disclosure of PHI, contact the HIPAA Privacy or Security Officer immediately.

• Do not remove PHI from Tufts MC campus unless absolutely necessary.
  – If so, electronic data MUST be encrypted on the laptop or the mobile device, if physical data (paper), obtain permission from your department lead.
  – In transport, secure on your person, lock in a secure location, and do not expose to other parties.

• Employees are subject to disciplinary action and/or termination for violations of Tufts HIPAA data security policies
• Tufts MC has resources to clarify issues, answer questions and resolve conflicts/problems
  • HIPAA Hotline – 617-636-4422
  • Tufts Medical Center Privacy Officer – Jeffrey Weinstein
  • Tufts Medical Center Security Officer – Sonia E. Arista
  • TuftsMCISInformationSecurity@tuftsmedicalcenter.org

• Confidential reports of suspected violations may be made by calling 6-2815.