GUIDANCE (Oct. 23, 2006)

Updated: February 2010

HIPAA BACKGROUND

HIPAA was enacted as a broad Congressional attempt at healthcare reform - it was initially introduced in Congress as the Kennedy-Kassebaum Bill. The landmark Act was passed in 1996 with two objectives.

1. One was to ensure that individuals would be able to maintain their health insurance between jobs. This is the Health Insurance Portability part of the Act. It is relatively straightforward, and has been successfully implemented.
2. The second part of the Act is the "Accountability" portion. This section is designed to ensure the security and confidentiality of patient information/data. In addition, it mandates uniform standards for electronic data transmission of administrative and financial data relating to patient health information.

This document presents a summary of the second part of the legislation.

For specific information and guidance on policies and procedures for complying with HIPAA, please see our **Faculty & Staff - Guidance** section.

The Standards

The HIPAA legislation required the **Department of Health and Human Services** (DHHS) to broadcast regulations on the specific areas of HIPAA, called the Rules. These Rules were finalized at various times and health care organizations had 2 or 3 years (depending on size) to comply with the specific requirements.

The Rules are composed of Standards. The HIPAA Standards resulted from many years of public and private sector collaboration. Industry workgroups were formed and reports written with recommendations on how to better manage and protect health information. The goal of this initiative was to define uniform standards for transferring health information among healthcare providers, health plans, and clearinghouses (covered entities) while securing health information and ensuring patient privacy and confidentiality.

Rule	Definition	Compliance Deadline
Transactions and Code Sets	• nine encounter related transactions • diagnostic, therapeutic, and treatment codes	October 16, 2003
	Health Claims Attachments	TBD
Identifiers	Employer Identifier Standard	July 30, 2004
	National Provider Identifier Standard	May 23, 2007
	Health Plan Identifier Standard	TBD
	Individual Identifier Standard	TBD
Privacy	defined as controlling who is authorized to access information. Better said, it is the right of individuals to	April 14, 2003

	keep information about themselves from being disclosed.	
Security	defined as the ability to control access to, and prevent information from accidental or intentional disclosure to unauthorized persons; and, from alteration, destruction, or loss.	April 20, 2005

Click here to view the **University of Chicago Medical Center Organizational Contacts**.

Who is Affected by HIPAA?
HIPAA applies to health plans, healthcare clearinghouses, and to healthcare providers that electronically transmit health information in connection with standard transactions.

"Health plan" generally includes any individual or group plan, private or governmental that provides or pays for medical care. Employee health benefit plans are excluded if they are self-administered and have fewer than 50 participants. Government-funded programs are excluded if their principal purpose is something other than providing or paying for health care, or if their principal activity is the direct provision of health care or the making of grants to fund health care.

"Healthcare clearinghouse" is a public or private entity that processes health information received from another entity, or converts transactions from non-standard into standard format, or vice versa. The regulations distinguish between a clearinghouse dealing with information in its own right (in which case it is bound by all the requirements of the regulations), and in its capacity as a business associate of another covered entity (in which case some of the requirements do not apply, but it is bound by its business associate contract with the covered entity). For example, the patient rights provisions would be enforced through the business associate contract, not directly.

"Healthcare provider" is any person or organization who furnishes, bills, or is paid for health care in the normal course of business. **However, healthcare providers are covered by the rules only if they transmit electronic health information in connection with a standard transaction.**

An entity that fits more than one definition must comply with the rules as they affect each of its functions, and may use or disclose information only as appropriate to the function for which the use or disclosure is made.

All health plans, claims clearinghouses, and health care providers that choose to transmit any of the transactions in electronic form must comply within 24 months after the effective date of each final rule (small health plans have 36 months).

HIPAA Requirements - *Transactions and Code Sets Standards*
Compliance Date - October 17, 2002

Many healthcare providers and health plans used EDI (Electronic Data Interchange) or the digital exchange of standard business documents and data. Electronic Transactions were so prevalent that the DHHS estimated that 400 different formats were being used to process health care claims. This lack of standardization makes it difficult for vendors to develop software solutions, decreases potential efficiencies, and increases costs for healthcare providers and health plans.

The widely adopted use of standards is required to perform EDI using a common interchange and data structure. Under HIPAA, DHHS was directed to issue standards for electronic data transactions used in administering healthcare data and information. Using industry-wide standards eliminates the need for software adaptation for multiple formats required to meet the demand of proprietary information systems, now being used by providers and health plans. Operational efficiencies with long-term savings are the anticipated results.

The HIPAA Standard EDI format requires standardization of the data content by specifying uniform definitions of

the data elements that will be exchanged in each type of electronic transaction and identification of the specific codes or values that are valid for each data element. Standards were adopted for the following administrative and financial health care transactions:

1. Health claims and equivalent encounter information.
2. Enrollment and disenrollment in a health plan.
3. Eligibility for a health plan.
4. Health care payment and remittance advice.
5. Health plan premium payments.
6. Health claim status.
7. Referral certification and authorization.
8. Coordination of benefits.
9. First report of injury.

All providers, clearinghouses, and health plans that exchange transactions electronically are required to modify existing or install new information systems to incorporate the data requirements for the new transaction standards, and use the medical and non-medical code sets.

HIPAA Requirements - *Privacy*
Compliance Date - April 14, 2003

Very few people are going to argue that ensuring the privacy of protected health information (PHI) is not important. Every individual has the right to know that his/her information is not going to be released to just anyone. Numerous examples exist regarding what can happen when personal information finds its way to a third party in an unauthorized manner. It can mean tremendous headache and heartache for the individual. Moreover, if organizations fail to ensure the confidentiality of patient information it can lead to financial and legal repercussions as well as the loss of public trust.

The Basics...

What is Protected Health Information (PHI)?
This information is any individually identified health information including demographic information that relates to the individual's past, present, or future physical or mental health condition or any other identifying information that can be used to identify the individual. The Privacy Rule states that the following identifiers are considered PHI and must be protected:

1. Names
2. Address (including zip code)
3. Dates (birth, admission, discharge, death)
4. Telephone numbers
5. Fax numbers
6. E-mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/License numbers
12. Vehicle identifiers and serial numbers (including license plate)
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses

16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

PHI is part of everything you do. It exists in verbal and written communication, interactions with technology (i.e. faxing, dictation) and activities related to the privacy rules. For example, we come in contact with a patient's health information when we speak to a colleague about a patient's treatment, review a patient's medical record or bill and when you access information using a computer.

Use and Disclosure
Under the Privacy Rule, we may use and disclose PHI without patient written authorization for the purposes of ***treatment, payment, and health care operations***. ***Treatment*** is the provision, coordination, and/or management of a patient's condition through diagnostic testing, referral for services in another specialty, and consultations between providers.

Payment refers to the activities of reimbursement for services, communication with insurers or others involved in the reimbursement process. This area also includes eligibility verification and billing and collection.

Health Care Operations pertains to all other areas including quality assurance activities, competency activities, residency and medical school programs, conducting audit programs for compliance, training programs for allied health, business planning and development to define only a few.

There are other situations in which information may be used or disclosed without the patient's authorization. Some of these areas include:

1. Workers Compensation
2. Law Enforcement Purposes
3. Victims of Abuse
4. Health Oversight Activities
5. Public Health Activities

Authorizations
Under the HIPAA Privacy Rule, organizations must obtain the patient's signature (authorization) for any use or disclosure outside of treatment, payment, and health care operations unless it is specifically identified as an area of exception based on the guidelines of the Privacy Rule. Specific authorizations are required for disclosure of:

1. Psychotherapy notes
2. Marketing (some exceptions)
3. Fund Raising
4. Research

Incidental Disclosure
The HIPAA Privacy Rule is not intended to prohibit the patients' treatment team from talking to each other and/or to their patients. Of course, others outside the treatment team may be present during these discussions. While reasonable precautions should be used to avoid sharing patient information with those not involved in the patient's care, it is possible that minor amounts of patient information may be disclosed to people near where patient care is delivered or being coordinated. This is referred to as an incidental disclosure. Privacy principles do not prohibit an incidental disclosure of patient information so long as reasonable safeguards are taken to minimize the disclosure. What is reasonable depends on the situation.

Minimum Necessary and Need to Know
The PHI you need to do your job is called "minimum necessary." It is information you "need to know" to do your job. Despite safeguards and controls to minimize access, we know that PHI surrounds us. If you come into contact with PHI and your job does not require it, you should not discuss or use this information.

Notice of Privacy Practices
The Privacy Rule requires healthcare facilities to provide patients with a notice advising them of their rights and telling them how their PHI may be used or disclosed. This is called the Notice of Privacy Practices. Every patient is required to receive the Notice on the initial visit to the hospital. The Notice provides patients with information regarding their rights under the Privacy Rule. The patient has the right to:

- Access their own records and obtain copies.
- Ask to amend or correct any inaccurate or incomplete PHI.
- Request a restriction limiting access to or disclosure of PHI.
- Request an accounting of how their PHI has been disclosed.
- Receive written notice of how their PHI may be used or disclosed.
- File a complaint if they believe their privacy has been violated.

Breach Notification
In February 2009, the Health Information Technology for Economic and Clinical Health ("HITECH") was enacted as part of the American Recovery and Reinvestment Act of 2009 ("ARRA"). HITECH makes significant changes to HIPAA's administrative simplification provisions pertaining to privacy and security, including notifying individuals (and in some instances, media outlets) when there has been a privacy/security breach.

Previously, covered entities (health care providers, health plans and health care clearinghouses) were obligated to mitigate harm caused by authorized disclosures of protected health information ("PHI"), but not required to give notice to the individuals whose information was inappropriately disclosed. With HITECH, covered entities and business associates will be required to notify individuals when security breaches occur with respect to "unsecured" information. Unsecured information means information not protected through technology or methods designated by the federal government. In addition, if the breach involves 500 or more individuals, notice to the U.S. Department of Health and Human Services and the media is also required.

What is a breach? Under the HITECH regulations, a "breach" is the unauthorized acquisition, access, use or disclosure of PHI that compromises the security and privacy of the PHI. "Compromise the security and privacy of the PHI" means that the breach poses a significant risk of financial, reputational or other harm to the individual.

Time Frame. Covered entities need to notify an individual of a breach of his/her PHI "without unreasonable delay" or no later than 60 days after the breach. A covered entity is considered to have become aware of the breach when the first workforce member or business associate first knew of the breach. *Because of this quick time frame, all UCMC employees and faculty need to be aware of these breach notification provisions and continue to report breaches to the HIPAA Program Office as soon as they are discovered.*

Complaints and Enforcement
We must have a procedure to address patient complaints. Patients can contact the HIPAA Program Office to make a complaint as well as contact the Federal Government Agency in charge of enforcing the HIPAA Privacy Rule - **The Office of Civil Rights**.

Civil penalties for not obeying the Privacy Rule are tiered based on increasing levels of culpability:

Violation	Each Violation	Multiple Violations in same year
Violations occurred without the knowledge of covered entity and by exercising reasonable diligence would not have known it violated the HIPAA Privacy Rule	$100-$50,000	$1,500,000
Violations due to reasonable cause	$1,000 to $50,000	$1,500,000

Violations due to willful neglect but are corrected within 30 days	$10,000 to $50,000	$1,500,000
Violations due to willful neglect and are not corrected	$50,000	$1,500,000

Criminal penalties for a person who knowingly violates HIPAA are as follows:

- $50,000 and a one year prison term
- $100,000 and up to 5 years in prison for wrongful conduct involving false pretenses
- $250,000 and up to 10 years in prison for wrongful conduct with intent to sell, transfer, or use individually identified health information for personal gain or malicious harm.

HIPAA Requirements - *Security*
Compliance Date - April 20, 2005

The HIPAA Security Rule became effective on April 20, 2005. The Security Rule standards define how we are to ensure the integrity, confidentiality, and availability of our patients' electronic protected health information (ePHI). The Security Rule requires that we have administrative, physical, and technical safeguards for protecting ePHI. Some examples of each are:

Administrative Safeguards: administrative functions that should be implemented to meet the security requirements.

1. Assigning or delegating security responsibility to an individual - Chief Security Officer.
2. Training workforce members on security principles and organizational policies/procedures.
3. Terminating workforce members' access to information systems.
4. Reporting and responding to security incidents.

Physical Safeguards: mechanisms to protect electronic systems, equipment, and the data they hold, from threats, environmental hazards and unauthorized intrusion.

1. Limiting physical access to information systems containing ePHI (i.e. server rooms).
2. Preventing inappropriate viewing of ePHI on computers.
3. Properly removing ePHI from computers before disposing or reusing them.
4. Backing up and storing ePHI.

Technical Safeguards: automated processes used to protect data and control access to data.

1. Providing users with unique identifiers for accessing ePHI.
2. Accessing ePHI during an emergency.
3. Encrypting ePHI during transmission.
4. Automatically logging off users after a determined time period.

Patient Privacy/Security and Technology
As we use technology to improve patient care, we are faced with additional challenges to protect patient

information from unauthorized use and disclosure. It is important to understand the form of technology being used and the precautions we must take to safeguard patient information.

Conclusion

Our patients entrust us with their health information; therefore we must protect it against deliberate or inadvertent misuse or disclosure. The consequences of not complying with HIPAA are too great. We do not want to see the University of Chicago Medical Center's name in the newspaper associated with a systems attack or theft of patient information. So, it is imperative that we all follow our privacy and information security policies, and do the right thing... protect our patients' privacy and confidentiality of their health information