BE HIP ON HIPAA

Health Insurance Portability & Accountability Act of 1996

Regulatory Issues in Laboratory Management
February 12, 2008
Presented by:
Jeniece Poole, CIPP/G
U of A Privacy Officer

HIPAA Privacy & Confidentiality of Protected Health Information
Understanding YOUR responsibilities

Why Was HIPAA Created?
- To establish minimum federal standards for safeguarding the privacy of individually identifiable health information

What is HIPAA?
- HIPAA is the Health Insurance Portability and Accountability Act of 1996 (PL 104-191)
- Also referred to as the Kennedy-Kassebaum Act
- HIPAA was enacted by the federal government on August 21, 1996 with the intent to assure health insurance portability, reduce healthcare fraud and abuse, guarantee security and privacy of health information and enforce standards for health information.

The History of HIPAA
- Regulation has 3 areas of focus
  - Portability of/ and access to Health Benefits
  - Preventing Fraud and Abuse
  - Administrative Simplification
HIPAA Regulations were designed to:
- Assure continuity of coverage between health care plans/insurance carriers
- Accountability for fraud and abuse
- Protect Individuals’ rights to privacy and confidentiality
- Assure the security of electronic transfer of personal information

Fraud and Abuse
- HIPAA expands the False Claims Act to include healthcare claims and
- Intentional fraud is a criminal act
- To be guilty of fraud, you need only to engage in a pattern or practice of presenting claims that you know will lead to greater payment

Teaching Hospital Physician’s Fraud OIG Sanctions
- Teaching Hospital Physicians’ Fraud
- A four year investigation into billing practices in the University of Washington Medical System ended with the University's physician practice plans agreeing to pay $35 million in restitution, damages and penalties to the state and federal governments for over billing Medicare and Medicaid. This FCA settlement is the largest ever paid by a practice group related to a teaching hospital for failing to comply with Federal billing regulations. As a result of the investigation, two University physicians were convicted of criminal charges in connection with the fraud, and a former University neurosurgeon pleaded guilty to obstruction of a Federal criminal health care investigation. In addition, a University-affiliated nephrologist pleaded guilty to health care billing fraud and admitted engaging in fraudulent conduct spanning approximately 11 years during which the defendant wrote notes in patients’ dialysis records indicating that he was present when he was not.

Fraud and Abuse in Billing Practices is Serious Business
- U of A Dermatology Clinic dismissed two physicians who were found in violation of the Medicare regulations
- Medicare was billed for services where the resident examined the patient and treatment was billed as if the physician was providing the care
- CMS has not made any formal decisions as to findings and penalties

HIPAA aka Administrative Simplification Rule
- Includes:
  - EDI (Electronic Data Interchange)
  - Privacy
  - Security
  - Unique Identifiers
Privacy (Effective 04/14/03)

- Requires Covered Entities to safeguard patient health care information
  - Covered Entities are defined as:
    - Health Care Providers
    - Health Care Plans
    - Health Care Clearinghouses

EDI (Effective 10/16/03)

Electronic Transmission of healthcare data transferred or received
- Most commonly used for claims processing and payment
- Reduction in paper transactions
- Reduces risk of lost paper documents

Security (Effective 04/21/05)

- Intricate interaction of all aspects of our information systems to insure the protection of data
- Training, Technology, Administration and Physical Safeguards Required

PURPOSE

- Compliance with the rule involves implementation by a covered entity of policies and procedures to ensure the confidential use and disclosure of protected health information by all staff

What Does Protecting Personal Health Information Mean?

- Making sure it is private
- Making sure it is accessible to the appropriate provider
- Making sure it is safeguarded from unauthorized users
- Educating healthcare consumers

What Does Protecting Personal Health Information Mean?

- Making sure it is private
- Making sure it is accessible to the appropriate provider
- Making sure it is safeguarded from unauthorized users
- Educating healthcare consumers
Making Sure it is Private

- Establish and review privacy policies
- Communicate those policies to all employees
- Reinforce the policies by using day to day examples

Establish and Review Privacy Policies

- Reviewing policies – what to look for:
  - Review of state and federal laws for regulations that affect your policies
  - Review of the organization’s policies for privacy and security. Are they adequate?
  - Do they need clarifications?

Remember

- The term “HIPAA Privacy” refers to accessing and the sharing the patient’s Protected Health Information (PHI)….This is DATA.
  - HIPAA Privacy is CONFIDENTIALITY

Confidentiality

- Confidentiality refers to data, not to the person
- Confidentiality limits who can access the data
- Confidentiality defines how the data will be stored

Multiple Users May Access Health Information

- Admitting Clerks
- Caregivers from the ED to the morgue
- Physical Therapists
- Nutritionists
- Lab Personnel
- Pharmacists
- Receptionists in physician offices
- Transport Techs
- Respiratory Therapist
- Billing Clerks
- Insurance processors
- School personnel
- Home Health Agencies
- Medical Records Clerks
- Researchers
- Website Managers

Why do we need Health Care Privacy?

- Gives patients more control over their health information
- Sets boundaries on the use and disclosure of health records
- Establishes appropriate safeguards for all people who participate in or are associated with the provision of health care
- Holds violators accountable through civil and criminal penalties
What Happened before HIPAA?
- Various State Laws Applied
- No consistent rules
- Most states had privacy regulations
- Few states had financial resources to enforce strict compliance with regulations
- Arizona law for privacy and medical record safekeeping is over 150 years old

Real Life Examples
- In 1998, an Atlanta truck driver lost his job after his employer learned from his insurance company that he had sought treatment for a drinking problem
- The late tennis star, Arthur Ashe's HIV positive status was disclosed by a healthcare worker and published by a newspaper

Real Life Examples
- Tammy Wynette’s medical records were sold to the National Inquirer by a hospital employee for $2,610

Addressing Patient Concerns
- Are my records confidential?
- How will my privacy be protected?
- Who can access my diagnosis and treatment?
- How secure is my information that is transmitted over the internet?
- Where is my information stored?

What is patient health care information?
- Individually Identifiable Health Information (IIHI)
- Protected Health Information (PHI)
- Relates to the past, present or future physical or mental health condition of an individual

HIPAA Patient Rights
Individuals have the right to:
- Receive a Notice of Privacy Practices informing as to the uses or disclosures of PHI
- Know how the CE will use PHI
- Right to access and review his/her medical record or other information
- Right to request amendment or addendum to their PHI
**HIPAA Rights regarding PHI**

Individuals have the right to:
- Right to receive an accounting of disclosures made for purposes outside of treatment, payment or health care operations
- Right to consent to and control the use and disclosure of their PHI
- Right to request confidential communications
- Right to file a complaint

**Personal Identifiers**

- This information can be in various forms and must be protected:
  - Electronic
  - Paper
  - Oral

**Security and Privacy Rule Distinctions**

- Inextricably linked
- Protection of the privacy of the information depends on the security measures to protect the information
- The Security Rule applies to information in electronic form
- The Privacy Rule applies to information in any form

**What is PHI?**

**Protected Health Information**

Refers to ANY patient information in any form that:
1. Is created or received by a covered entity;
2. Relates to a patient’s health condition in the past, present or future;
3. And identifies the patient

**What are Personal Identifiers?**

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and equivalent geocodes, except for the initial five digits of a zip code to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers

**What is PHI?**

PHI is ANY information transmitted or maintained in any form, such as prescription records, patient profiles, and oral communications on the phone or during patient counseling.
More Personal Identifiers

9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URL)
15. Biometric identifiers, including finger or voice prints
16. Full face photographic images and any comparable images
17. Internet protocol address numbers
18. Any other unique identifying number characteristic or code

What if I don’t want to share my health information?

- Each Notice of Privacy Practices contains information on who will be able to view your PHI, how it is shared and how it maintained
- It is assumed that you agree with the provisions of the NOPP
- If you do not want to share your information, you may exercise the opt-out option

Defining USE and DISCLOSURE

USE = Sharing of PHI within an entity or component
DISCLOSURE = Sharing of PHI outside an entity or component

Under HIPAA, patients have the rights to request a complete listing of ALL disclosures of PHI for 6 years

Confidentiality

- Role based access to PHI...Must have a need to know
- Do not share information with anyone, including co-workers, other patients, patient’s visitors or others who do not need to know.
- Limited to responsibilities defined in your job description--“minimum necessary” [does not apply to uses and disclosures for treatment]
  - Do you need this information in order to do your job?
  - What is the least amount of this information you need to do your job?

Confidentiality

- You should not use patients’ protected health information or share it with anyone, including coworkers, other patients, patient visitors or anyone else who may ask you about it who does not need to know.
- You should not share passwords or allow coworkers to use your computer access to input, review or obtain patient information.
What exactly must be done under the HIPAA Privacy Rule?

- Create a notice of privacy practices and provide it to all patients at time of entry into the company system
- Document that the patient received the notice—"good faith effort"
- Post the notice of privacy practices
- Provide mechanisms to ensure the patient rights identified in this rule
- Identify a Privacy Officer
- Implement "reasonable" safeguards that will protect patient privacy and guarantee confidentiality
- Train all staff on privacy obligations
- Create policies and procedures for the implementation of the privacy rule.

Violating privacy and confidentiality policies may result in

- Disciplinary action up to and including termination
- Criminal prosecution

HIPAA Violations/Penalties

- HIPAA specifies the penalties for misuse of personal identifiers
- PERSONAL as well as INSTITUTIONAL liability
- Civil Penalties: $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated

Penalties

Criminal Penalties

- Up to $50,000 and one year in prison for obtaining or disclosing protected health information
- Up to $100,000 and up to 5 yrs in prison for obtaining protected health information under "false pretenses"
- Up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm

Regulatory Oversight

- HIPAA regulations are administered by the Department of Health and Human Services
- Office of Civil Rights (OCR) is the designated federal agency for interpretation of regulation & determining compliance
- OCR receives and investigates allegations of privacy breaches
- OCR will conduct investigations and assess fines

Your Responsibilities

- Be sensitive
- Respect right to privacy
- Know company policies
- Implement reasonable safeguards
- Curb human nature
  - Curiosity
  - Sharing
- Participate in Training
- Sign the Confidentiality Agreement
- Follow the Code of Conduct
- Report privacy concerns and violations
**Incidental Disclosures**

- Overhearing a conversation among health care providers about a patient’s treatment;
- Walking past a computer displaying a patient’s information;
- Patients in waiting rooms overhearing patient names being called;
- Seeing patient names on sign-in sheets.

**DEVELOP GOOD HIPAA HABITS**

- Utilize security techniques when handling PHI
  - Don’t share passwords
  - Change passwords frequently
  - Don’t leave patient data on screens
  - Don’t leave charts open
  - Shred printed documents with patient data
  - Watch what you say in public areas

**GOOD HIPAA PRACTICES**

- Security measures cont’d
  - Only access patient data that you have a need to know to do your job
  - Avoid gossip situations
  - Report known or suspected breaches
  - Do not leave voicemails with sensitive patient information

- Do not leave PHI in or around copy machines/rooms
- Do not leave medical records / x-rays open in view of the public
- Avoid inadvertent disclosures among professionals
- Be careful with patient lists
- Be aware of company FAX and E-mail policies regarding the transmission of PHI

"Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either."
Workplace Example of Privacy

Let’s assume that Fred, an “employee” Community Medical Center, goes to the hospital lab for a blood test ordered by his physician. The results show that he is positive for the dreaded boogie virus. A half hour later the employee gets a phone call from a fellow employee (Humphrey, who works in janitorial services) who sends his condolences about the test results (he saw them posted on the Lab tech’s wall). Ten minutes later Fred receives flowers with a get well note from Nancy who works in Human Resources. Nancy tells the employee that the company’s medical plan needs to be altered because they just found out from Humphrey that Fred has the dreaded boogie virus. Then Wanda, from internal audit, calls and asks if there is anything else wrong because they heard about the boogie virus from Alfred in medical records - and by the way Alfred says your last x-ray looked suspicious. Humphrey & Nancy thought so too, and they want to send it to Felicia who works at the Pharmacy. Felicia called her buddy at the clinic and they have an ointment that will cure anything.

Contact Information

- Jeniece Poole, CIPP/G
  Privacy Officer
  University of Arizona
  Tucson, AZ 8572
  Office: 520 621-1465
  Fax: 520 621-1429

BE INFORMED

- http://arizona.edu
- http://vpr2.admin.arizona.edu/
- HIPAA/HIPAA.htm

Other websites:

- http://www.hhs.gov/ocr/hipaa
- http://security.arizona.edu
- http://www.irb.arizona.edu

QUESTIONS