usfcs
UNIVERSITY of SAN FRANCISCO
department of computer science

HIPAA

EJ Jung

11/17/2010

Federal laws

- National Institute of Standards and Technology, Computer Security Division http://csrc.nist.gov/index.html
- Federal Information Security Management Act of 2002 http://csrc.nist.gov/groups/SMA/fisma/
- HIPAA – Health Insurance Portability & Accountability Act of 1999
- FERPA – Family Education Rights & Privacy Act of 2004

usfCS
UNIVERSITY of SAN FRANCISCO
department of computer science

Causes of data leak

1. Stolen laptop
2. Virus or hack
3. Inadvertent posting of information on the Web
4. Stolen hard copies

HIPAA, The Real World

April 29, 2010

Debbie Thoman

Assistant Vice President for Compliance and Accreditation

University of Iowa Privacy Officer

University of Iowa Hospitals & Clinics
University of Iowa Health Care

HIPAA Privacy Rule:

Protecting Patient Privacy…It's Everyone's Responsibility

Why is patient privacy so important?

- **Patient Privacy Breaches are still in the headlines:**
  - Nurse in Arkansas fired and faces 10 yrs in prison/$250,000 fines for Wrongful Disclosure of PHI for personal gain/malicious harm
  - 27 hospital workers suspended without pay for 1 month for sneaking a peek at George Clooney's records
  - Confidential patient data sent to wrong company -- for 15 months
  - More than 300,000 patients' records stolen
  - 'Human error' exposes patients' Social Security numbers in N.C.
  - US Dept of Veterans Affairs loses 26 Million patients' records
  - Clerk at medical clinic in Florida left daughter unattended at workstation while signed on to system

Protected Health Information (PHI)

- **PHI** is defined by the Privacy Rule as "individually identifiable health information"

  (1) **individually identifiable** means "information that could reasonably identify an individual receiving healthcare services"

  (2) **health information** means "information related to the physical or mental health, healthcare or healthcare payment"

PHI Elements

Individually Identifiable

- Name
- Address
- Phone Number/Fax Number
- Medical Record Number
- Social Security Number
- Photograph
- Billing and other account numbers
- Date of Birth
- Date of Visit
- Fingerprints

Health Information

- Medical Charts
- Billing Information
- Lab Test Results
- X-Ray and Films
- Diagnosis and Treatment Records
- Flow Sheets

Patient Rights

The Privacy Rule grants patients the following rights with respect to their PHI*

1. Right to Access PHI
2. Right to a UIHC Privacy Notice
3. Right to Correct or Amend PHI
4. Right to an Accounting of Disclosures (Important)
5. Right to Opt Out of the UIHC Facility Directory
6. Right to Opt Out of Fundraising
7. Right to Request Restrictions to PHI
8. Right to Confidential Communications
9. Right to File a Complaint

**Prison inmates are excluded from these rights*

The Privacy Rule

- The Privacy Rule requires that UIHC staff safeguard the privacy of health information by:

  1) Limiting access to PHI to those involved in ***treatment***, ***payment***, or ***healthcare operations***

  2) Restricting access and disclosure in situations other than those listed above unless a specific exception exists as defined by the Privacy Rule or if specific consent is obtained from the patient

  3) Accessing health information on a "Need to Know" basis only – viewing only the minimal amount of PHI necessary to perform assigned functions

Minimum Necessary

What can staff access?

- Info you “need to know” to do their job

Does Minimum Necessary apply in every situation?

- Treatment – No, not for clinicians involved in care of patient
- Patients – No, they can access their PHI

How does the HIPAA Privacy Rule impact jobs?

Computer Security

- System passwords (IDX, INFORMM, IPR, CERNER) must be:
  - Kept secure,
  - Not shared, and
  - Changed regularly
- If possible, computer screens should not be kept in plain view
- **Always, always, always**…log off or close computer programs containing patient information when not in use
  - staff are responsible for all activity under their user name

How does the HIPAA Privacy Rule impact jobs?

Key Question:

- Prior to accessing, using, or disclosing any Protected Health Information (PHI), always ask this question:
- ***Do I need to access, use, or disclose this PHI to do my job?***
- If not, then do not access, use, or disclose

Scenarios

The names and facts in the following scenarios have been altered to protect the innocent (and the not so innocent). The scenarios are intended to provoke discussion of the basic principles that guide our evaluation of potential Privacy Rule violations.

Dining Out

You and your family are at a restaurant and you notice someone staring at you who seems very familiar. You approach the person and ask “Don’t I know you from somewhere?” The person becomes visibly uncomfortable and simultaneously you realize the person was a recent patient for whom you cared. What should you do?

A. Remind the patient that you met at the hospital while you were caring for him and ask him how he's doing.

B. Ask the person if he comes here often and what he recommends from the menu.

C. Politely say, "I must be mistaken, have a nice meal."

Big Dude Sports Star

Big Daddy, super sports star, is a patient in the hospital before he dies of injuries sustained in a car accident. Your friends are begging you to find out more information about what happened to Big Daddy. Your position gives you access to patient records in the computer and it would be easy to find out everything everyone is curious to know. Big Daddy won't know or care. He might even have been pleased to know that everyone is so concerned about him. Plus, some of the information will come out in the press in a few days anyway. What do you do?

Answer

A. Sneak a peek at the chart but refuse to share any information with friends.

B. Sneak a peek at the chart on your own personal time and share only information that will become public anyway.

C. Explain to friends that health care professionals cannot look at patient records without a good reason to know the information for health care or billing purposes.

D. Explain to friends that the institution has an audit system that will track anyone who looks at the patient's record and that you will lose your job unless you had a good reason to look at the chart.

Ross and Rachel

Ross and Rachel work together and are friends. They are such good friends that Ross often leaves his terminal without logging off of the system. Rachel has noticed this habit. On a particularly busy day Ross frequently needs leave his terminal. On one of these occasions, Rachel uses Ross's terminal to access her ex-husband Chandler's health information. Chandler runs an INFORMM "Show Staff Involved in My Care" report and sees Ross's name. He requests a full investigation. The tracking log confirms that Ross (or someone using his user ID) accessed Chandler's records. Ross is disciplined for inappropriate access. Is this fair?

Answer

- Yes; every employee is responsible for the access and activity that occurs under their user name and password in the electronic medical record systems. That is why you must never share your passwords and why you must always log off the systems or lock your personal workstation when not in use.

Concerned Ex-Husband

Your ex-wife receives her care at UIHC. She has a chronic heart problem and has hinted at refusing ongoing treatment. You have joint custody over three young children and are concerned that she might experience a heart attack while transporting the children to and from their activities. You have asked her about this issue several times and she refuses to discuss this with you. You just read an article in Reader's Digest about a man who had a heart attack on a Los Angeles freeway while his daughter was in the car. You are now very concerned and you consider looking at her appointment information just to make sure that she is keeping appointments with her cardiologist. Is this permissible?

Answer

- No; even though you may have good intentions of ensuring the safety of your children, this does not give you the right to access the records of your ex-spouse.

Patient Rights: Confidentiality

You had a very difficult day in the operating room and are deeply troubled that one of your patients almost died due to an unanticipated situation. You are concerned that you may not have recognized the signs of trouble soon enough and you need to discuss the case with someone you trust. At the end of the day you go home and share your difficult day with your partner. Have you violated the HIPAA Rule?

Patient Rights: Confidentiality

A. Yes. HIPAA prohibits the sharing of any patient information except for treatment, payment, or health care operations.

B. No. Clinicians must be able to vent to loved ones at the end of the day to preserve their mental health.

C. Maybe. It depends on the level of detailed information that was shared with the partner. No information that could identify the patient clinically, physically, or socially should have been shared. All individuals need to be able to vent and share troubles at the end of a difficult day. Perhaps sharing the details with a colleague involved in the case is a better option. If no information of sufficient detail to identify the patient was shared this would not be a violation.