Health Management Associates, Inc.

Annual HIPAA Training & Education (2005-2006)

*This training is to ensure all workforce (employees, volunteers and students) at **Santa Rosa Medical Center** understand the HIPAA Policies & Procedures of the hospital and HMA.*

Your HIPAA Officers!

- ***HIPAA Privacy Officer:***

Angela A. Dreading

626-5160

- ***HIPAA Security Officer:***

Marie Howatt

626-5003

What is HIPAA?

(Health Insurance Portability & Accountability Act of 1996)

HIPAA is a broad law dealing with the privacy and security of health information. There are two Rules contained in the law:

- *The Privacy Rule tells hospitals* ***when*** *and* ***how*** *they can* ***use or disclose*** *patient health information.*
- *The Security Rule tells hospitals* ***how to protect*** *health information from being inappropriately accessed, edited, or destroyed.*

What Is Protected Health Information (PHI)?

PHI is ALL personal health, billing and demographic information in ANY format (Oral, Paper, Picture or Electronic) CREATED OR HELD by the hospital.

Minimum Necessary *or* “Need to Know”

- *All members of the hospital workforce contribute to the care of the patient. That doesn’t mean everyone needs to see health information about patients.*

- *If you do not need to know confidential information to provide care (clinical or financial) you are* **NOT** *permitted to access it. This includes* your *PHI.*

Privacy and Security Rules: **Differences-**

Privacy Rule Regulates:

- *Use, Disclosure and Tracking of PHI*
- *Patient's Rights to their PHI:*
  - *Access*
  - *Amendment*
  - *Authorization Requirements*

Security Rule Regulates:

- *Computer hardware and software containing PHI*
- *Buildings that house computer hardware and software*
- *Who has access to data and how access to data is granted*
- *Visitor access to facility*

Employee Discipline: Policy 1.4

- *There are three different Groups of disciplinary action depending on the violation.*

- *The following examples show what can happen if you do not protect our patient’s information correctly:*

Group 1 Discipline:

1st Offense: Written Warning
2nd Offense (in 2 yrs): Suspension w/out pay
3rd Offense (in 2 yrs): Termination

Examples of Violations:

- *Not signing off computer (with PHI) when leaving a work area.*
- *Leaving confidential information displayed on computers, desks, workstations, or nursing stations where others can see it.*

Group 2 Discipline:

1st Offense: Written Warning or Suspension
2nd Offense (in 2 yrs): Termination

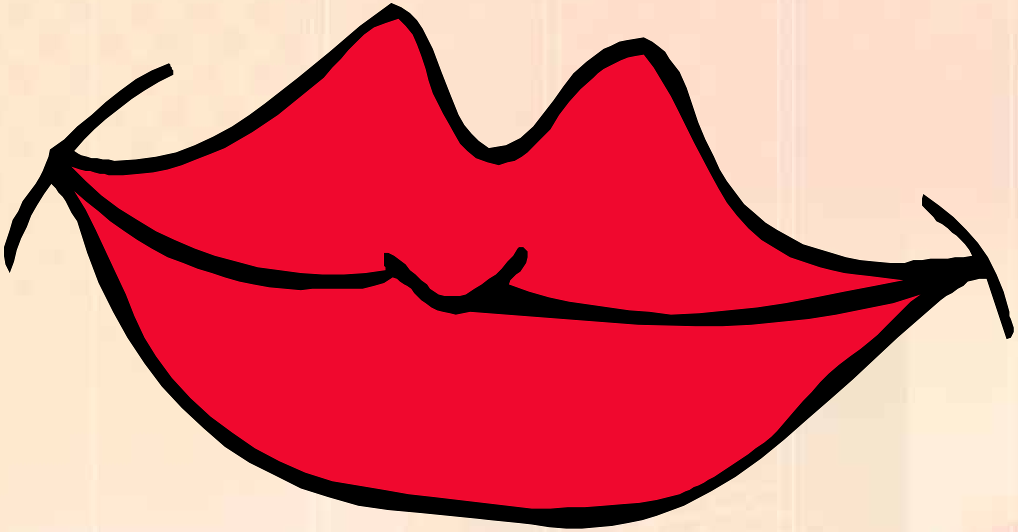
- *Accessing information (dates of births, telephone numbers, or addresses of people **not** needed to do your job.*
- *Sharing your password with a co-worker.*
- *Accessing confidential medical information on a patient you have no job-related responsibility for, including friends/family AND **your own** information!!!*

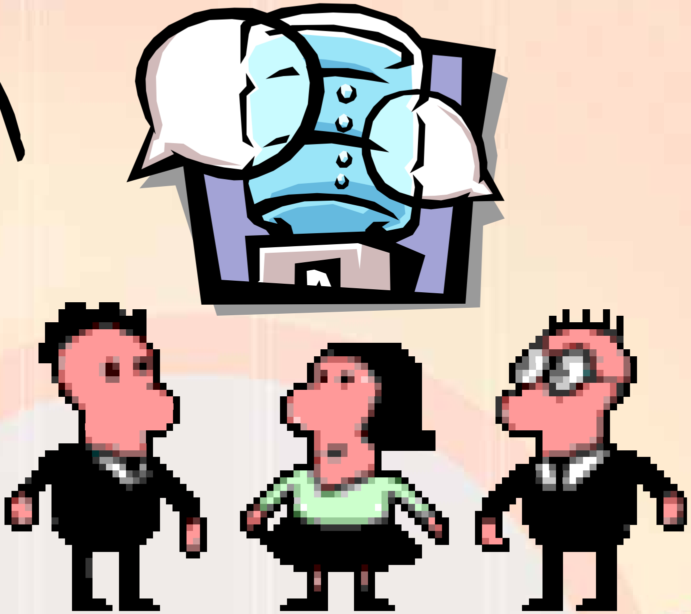
Group 3 Discipline:

1st Offense: Termination

- *Using a co-worker’s password without their knowledge.*
- ***Disclosure of PHI which you have accessed, without authorization and when NOT involved in the care of the patient.***
- *Releasing any PHI for personal gain or releasing PHI with intent to harm the reputation of the individual or our organization.*
- ***Accessing HIV test results, records of sexually assaulted or domestic violence victims when not involved in the care of those patients.***

#1 ISSUE *and* BIGGEST RISK!





How, you ask?

NOSY EMPLOYEES!!

- *A co-worker accesses information.* ***The only reason was for curiosity****:*
  - *Co-worker who is a patient*
  - *Physician who is a patient*
  - *Neighbors who are a patient*

Divulging information to others with no reason to know!

Complaint Statistics & Comparisons

HMA

as of 7/25/05

Complaints filed: 888

Confirmed violation: 529 (60%)

Suspensions: 29

Terminations: 26

Registered Nurse	*9 (35%)*
Clerical/Aide	*8 (31%)*
Other licensed	*7 (27%)*
Director	*1 (3.5%)*
LPN	*1 (3.5%)*

OCR

as of 8/31/05

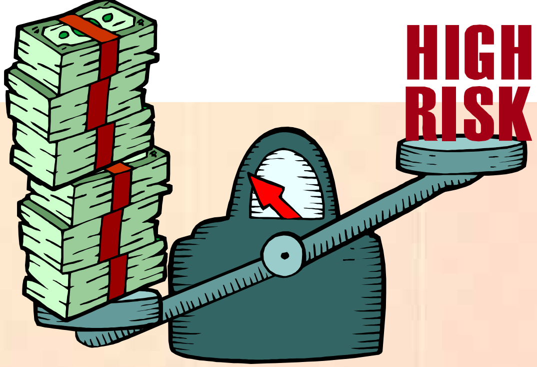
Complaints filed: 14,900

Resolved:10,132 (68%)

Remain open: 4,768 (32%)

DOJ referral: 231

Problem Areas…



- *Sensitive Health Information (HIV, Abuse, Psych)*
- *Minimum Necessary=“need to know”*
- *Inappropriate disclosure to **your** family/friends*
- *Access of employee’s own “patient” record*
- *Reporting of suspected violations*
- *Passwords*
  - *No sharing!*
- *Identity Verification (Policy 2.7)*

Civil Penalties

- *Imposed when policies not implemented/followed causing inappropriate, inadvertent disclosure.*
- *Fines of up to $100 for each violation of the law per person.*
- *A limit of $25,000 for each identical mistake.*

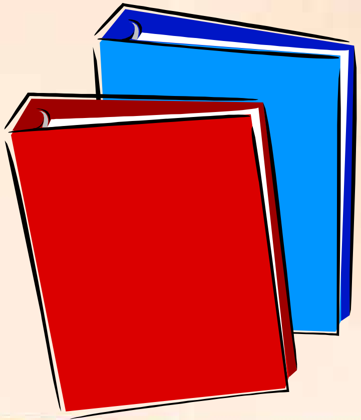
For instance, if a hospital released information on100 patients inappropriately, it could be fined $100 for each record, for a total of $10,000.

Criminal Penalties

- *Harmful intent to another person or entity by disclosing the information or having some personal gain.*
- *Can include large fines and jail time*
  - *selling patient information is worse than accidentally letting it be released, so it brings stiffer penalties.*
- ***Criminal Penalties can be as high as $250,000 and 10 years in prison.***

Where can I find information on HIPAA Policies?

Each department has a HIPAA Policy Manual.



HIPAA Privacy:

What you need to Know!

Reasonable Precautions to protect patient privacy include:

- *Closing room doors/drawing privacy curtains when discussing the care of a patient.*
- *Ensuring that medical records are not left where others can see or gain access to them.*
- *Keeping Laboratory, Radiology and other test results private.*
- *Keeping the fax machine out of view and using a coversheet.*
- *Making sure that the computer screen is not visible.*

Verification of Identity & Authority:

- *Before making any disclosure permitted by the Privacy Rule* you *must verify the identity of the person requesting PHI and that person's authority have access to it* ***if both are unknown to you.***

White Boards

- ***PHI on Whiteboard: Name or initials!!!***

  1. Must be out of public view.

  2. Can be in public view ***IF*** *in a restricted area. (ED, ICU, CCU, OR, Psych Unit, etc.)*

- ***No PHI, No problem!***

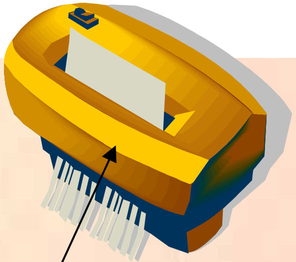
Can be in public view with the following:

- *Room #*
- *Doctor's Name*
- *Nurse's Name assigned to room*

Patient Directory

- *If visitors ask you for information about a patient, you need to check to be sure the patient has agreed to be listed in the directory and has not asked that information not be given out.*
- *The name of the patient must be known by the person asking for information. (It can't be… "that gentleman who was in that terrible accident on Interstate-10 last night..")*

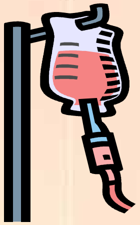
Destruction of PHI



- ***Trash must be checked!***
  Patient Name, Demographics are types of information that is protected!

  - *Patient Name bands*
  - *Telemetry Strips*

- ***What about IV Bags with med Labels?***



  -- If you can, peel Label. Label must be shredded.
  OR Black-out with marker and place in Red Bag trash.

Passwords

- *Your sign-on and password is your personal "key" to use the computer system.*
- *Do NOT share your password with anyone for any reason!*
- ***Audit trails will document who was where in our system.***
- ***You can be terminated (first offense) if you access information because you are being nosy!***
- ***HMA has zero tolerance for nosiness!***

It is always better to *ASK* for "*permission*" to disclose information than *BEG* for "*forgiveness*" after the fact!!

- *Patient MUST sign authorization for any disclosure EXCEPT for:*
  - *Treatment (including sending patient information to another health care provider)*
  - *Payment*
  - *Operations (State reporting, PI, etc.)*

Privacy Practices Notice

- *This notice tells patients about our privacy policies and practices.*
- *It describes the way we will use their information.*
- *It tells patients about their rights,*
  - ***to get their own records***
  - ***request amendments to them.***
- *We must make a “good faith” effort to obtain the patient’s written acknowledgement that they received a copy of the notice.*

HIPAA Security:

What you need to Know!

Information Access Management

- *All persons authorized to have access to PHI shall have a unique User ID.*
  - *This process shall include all volunteers, temporary workers and independent contractors.*
  - *Workforce members and other authorized users will be required to select passwords for each of their User IDs.*
  - *User IDs and Passwords should NEVER be shared!*

Log-in Monitoring

- *The hospital monitors log-on attempts to the hospital computer systems.*
- *An individual’s access shall be restored only after the person’s identity has been verified (in person).*
- *If you are locked out of the system because you forgot your password, please contact your supervisor.*

Access Control

- *The Security Rule requires facilities to implement access controls to the physical plant - in other words, doors need to be locked or manned.*
- *The policies discuss a variety of types of people who have access to the facility such as Patients, Visitors, Volunteers, Staff, and Physicians. You **MUST** wear your identification badge at all times!*

Facility Security Plan

- *Public Access.*   *All entrances in which public access to the Hospital is allowed shall be manned by reception or security personnel.*
  - *The public access areas are:*
  - *ED Entrance-24 hours per day*
  - *Main Lobby Entrance-7a.m.-9 p.m.*

Facility Security Plan

- *Non-public Access. All non-public entrances shall be locked or secured in some manner so as to prohibit entrance without proper authorization.*
- *Non-public Access areas will be locked and on (indicate security method) access:*
  - *Back door leading to Locklin Building*
  - *Door by Maintenance Dept.*
  - *Door by vending machines*
  - *Administration Stairwell*
  - *Physician Dictation Lounge-1st floor*

Facility Security Plan

- *ALL other entrances to the hospital will be locked - you will still be able to exit the building through these doors but will NOT be able to access the building through these doors.*
- *ANY staff person found tampering with the door security system (propping open doors, opening doors for others) will be subject to disciplinary action* ***up to and including termination.***

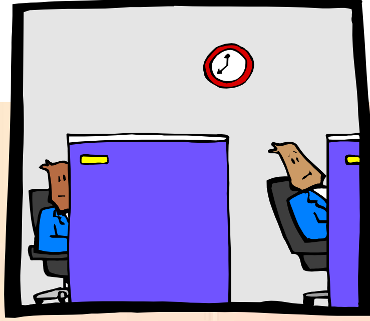
Visitor Identification

- *All staff MUST question visitors or other persons who are in restricted areas and are not displaying proper identification.*
- *Vendors and contractors will be wearing their company ID in addition to hospital identification noting that they have permission to be in the building.*
- *Volunteers and Physicians MUST wear their identification badge as issued by the hospital.*

Workstation Security at Off-Site Locations:

- *If the hospital allows you to perform some or all of your work from an off-site location, you are responsible for the privacy and security of all materials. This includes, but is not limited to:*
  - *Patient Charts*
  - *Computers*
  - *All confidential working papers*
- *Keep in a location not accessible to others!*

Audit Controls



IMPORTANT!!

- *Audit trails will document who was where in our systems and will document what the employee was accessing. This is performed by our HIPAA Officers (Privacy & Security). Your User ID will link to every item read or printed.*

- *Every employee, physician and VIP admitted to our hospital will have their account reviewed for inappropriate access.*

- *Disciplinary action will be taken if employees are found violating HIPAA policies and accessing information that they have no need to know.*

Security Incident Procedures

- *If you suspect your computer has received a virus, contact your Privacy Officer, Risk Manager, and IS Director immediately.*

- ***No** software can be loaded onto computers without the permission of the IS Director!*

- *This includes downloads from the Internet!*

Reporting Violations

We expect all employees to adhere to the privacy and security policies, but we know there may be times when the policy is being abused.

- ***Report violations or suspected violations to the Privacy Officer or HIPAA Security Official.***
- ***You may report anonymously, if you wish.***
  - ***HMA Compliance Hotline, PO Box #***
- ***You will not be retaliated against if you report a privacy violation.***
- ***It is part of your job to report instances where you suspect policies are being broken.***

Conclusion:

- *We must all remember to protect the privacy and security of patient information at all times.*
- *We are all patients from time to time. How would you feel if your own health information was used or disclosed in a way that was harmful to you or your family?*
- *If you have a question about HIPAA, ask your supervisor or your Privacy or Security Officer.*

Thank You for your Attention!

- *To complete your training, please take the quiz associated with this module.*

- *You must complete a HIPAA Training Certificate at the end of this training!*