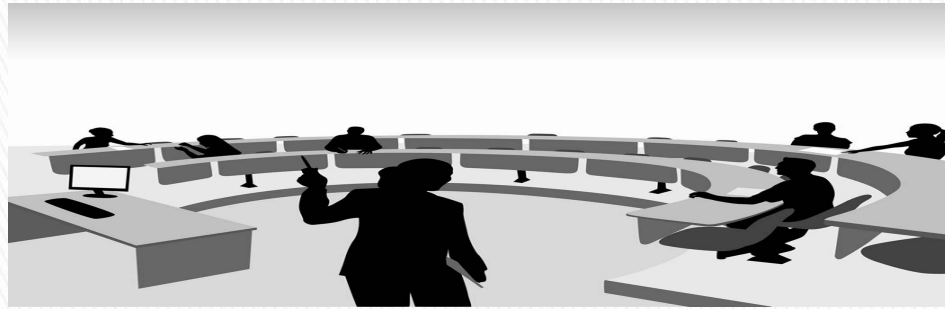




Health Management  
Associates

# HIPAA Training 2009





This training is to ensure all workforce (associates, volunteers and students) understand the HIPAA Policies and Procedures of Health Management Associates hospitals and physician practices.



# What is HIPAA?

*(Health Insurance Portability & Accountability Act of 1996)*

HIPAA is a broad law dealing with the privacy and security of health information:

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

# Your HIPAA Officers:

▶ The HIPAA Privacy Officer is your HIM Director

▶ The HIPAA Security Officer is your Risk Manager



# First Essential Element of HIPAA: PHI



- ▶ Protected Health Information (PHI) is ALL PERSONAL HEALTH, BILLING AND DEMOGRAPHIC INFORMATION, IN ANY FORMAT (Oral, Paper, Picture or Electronic) CREATED OR HELD BY A COVERED ENTITY (hospital or physician, payer)
  - *(includes past, present and future healthcare)*

# Minimum Necessary or “Need to Know”



- ▶ All members of the 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.

# Our #1 Biggest Risk— NOSY EMPLOYEES!!

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

**Divulging information to others  
with no reason to know!**



# Problem Areas...



- ▶ Taking pictures of any patient's image, body part or X-ray with personal cell phone cameras (this will be grounds for termination)
- ▶ Access of sensitive health information (HIV, Abuse, Psych)
- ▶ Access of associate's own "patient" record in the computer system
- ▶ Passwords are not to be shared for any reason!
- ▶ Be sure you know who you're talking to when you disclose PHI

## Criminal Penalties:

These are Group 3 HIPAA violations and will be cause for termination



- ▶ Stealing and selling information about our patients.
- ▶ Causing harm to another person or entity by disclosing information about patients to someone who had no reason to have the information.
- ▶ 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?

HIPAA Policy & Procedure Manuals are located:

1. On-line at your facility's "Intranet" site
2. At the Health Management Associates corporate "Intranet" site @ [HMA-info.com](http://HMA-info.com)

# Patient Directory (Applies to hospitals only)



Directory information includes location or room number confirmation.

- ▶ If visitors ask you to confirm if a patient has been admitted you need to check to be sure the patient has agreed to be listed in the directory and has not asked that information be kept private.
- ▶ NO information can be provided if the patient has requested “Privacy” or “Top Secret Status”
- ▶ The name of the patient must be known by the person asking for information.

# 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.
- ▶ All associates, volunteers and other workforce members **MUST** wear their identification badge as issued by the hospital.

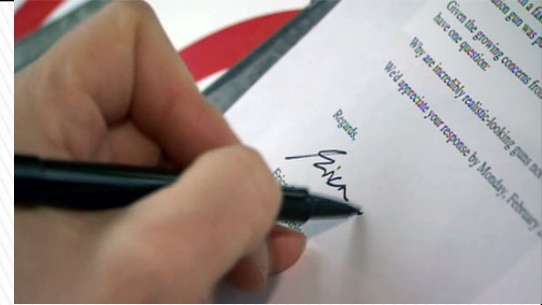
# Audit Controls



## IMPORTANT!!

- ▶ Every associate, physician and VIP admitted to our hospital will have their account reviewed for inappropriate access.
- ▶ Disciplinary action will be taken if associates are found violating HIPAA policies and accessing information that they have no need to know.
- ▶ Audit trails will document who was where in our systems and will document what the associate was accessing. This is performed by our HIPAA Officers (Privacy & Security). Your User ID will link to every item read or printed.

# Notification to Patients



- ▶ Starting 9/23/09, Federal law requires us to tell patients if someone has snooped into their information protected by HIPAA.
- ▶ We must also notify patients any time their protected health information was inappropriately disclosed outside of the facility, or if it was stolen or breached.
- ▶ We are required by the new HIPAA law to notify the patient in writing and report to the Federal Government.



- ▶ At any one time, if there are more than 500 patients who have their records snooped into or, if their protected health information is disclosed in any way outside of our facility, we must notify every patient and the Federal Government immediately.
- ▶ We may also need to notify the local media if 500 or more of the patients are from the same state.



© 2008 TOM FOTY

- ▶ We audit the accounts of our associates, physicians and VIPs to see if anyone snooped. If it was you, you will be suspended or possibly terminated.
- ▶ We audit random patient records to see if anyone was looking at information when they had no right to be in the record.



- ▶ associates cannot snoop on each other when they come into the hospital for clinical care.
- ▶ It doesn't matter if it is for lab work, diagnostic testing or for an admission.
- ▶ Remember, if you snoop, we WILL catch you.

# Who do we need to notify if a breach of PHI is detected?



- ▶ All of the affected patients.
- ▶ The Federal Government.
- ▶ Local media if 500 or more patients in the same area are affected.

# What is a breach?



- ▶ Under the Notification Rule, a breach means the:
  - Intentional Acquisition
  - Intentional Access
  - Intentional Use or;
  - Intentional & Unintentional Disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

# Examples of Breaches



- ▶ Lost laptop or PDA
- ▶ PHI left in the cafeteria, lounge, or public area
- ▶ “Snooping”
- ▶ “Cell phone pictures”
- ▶ PHI faxed to the wrong fax number or emailed to the wrong address or printed to the wrong printer
- ▶ PHI thrown into regular trash
- ▶ Information intended for one patient handed to another patient (not verifying your work).

# Reporting Deadlines for Notification



- ▶ Once we discover a breach of PHI, we have no more than 60 days to comply with the Rule's notification requirement – sometimes sooner.
- ▶ You should immediately report all suspected PHI breaches to the Privacy Officer.
- ▶ The Privacy Officer will need to conduct a full investigation.
- ▶ Determination will need to be made if a breach occurred and notification is required.

# What are the common causes of HIPAA violations

- ▶ “Snooping”
- ▶ Not checking your work (giving the wrong information to the wrong patient, incorrect fax number or email address)
- ▶ Patient information placed in the regular trash
- ▶ Lost or stolen laptop
- ▶ Cell phone or personal camera pictures of patient’s body parts or X-rays
- ▶ Thinking you won’t get caught!
- ▶ Forgetting how you would like to be treated if it were you!

# New Enforcement Actions Could Directly Affect You!



- ▶ If you are found to be responsible for any type of a HIPAA violation that the State Attorney General believes has threatened or in some way harmed a patient who is a resident of your State, you can be held responsible for your actions.
- ▶ The State Attorney General can bring a civil action in federal court against you!

## 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.



# Reporting Violations



- ▶ We expect all associates 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.
  - Health Management Associates Compliance Helpline: 1-888-462-0380
  - Health Management Associates, Inc. PO Box 770621, Naples, FL 34107
- ▶ 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.