# HIPAA Privacy and Security

*Mandy Rand*, IT Manager / HIPAA Security Officer

Madison County
Memorial Hospital

# What IS HIPAA ?

- The Health Insurance Portability and Accountability Act is a federal law that protects the privacy and security of patients’ health information

The Privacy Rule provides for the protection of patient privacy and grants patients certain rights regarding their health information

The Security Rule provides for the security of electronically stored health information

**How does HIPAA affect me?**

MCMH requires ALL workforce members to sign the MCMH Confidentiality Agreement, and work together to protect the confidentiality and security of patient, proprietary, and other confidential information

*“Confidentiality is everyone’s **JOB**, not everyone’s business”*

**Protected Health Information (PHI)**

Applies to health information in all forms:

Written

Spoken

Electronic

Photographic

Etc

Identifiers that apply to patients, their families, household members and employers:

- Name
- Address (Street Address, City, County, Zip Code, or other Geographic Codes
- Dates related to Patient (DOB, DOS, etc)
- Age Greater than 89 (Due to The fact that >90 years of age Population is relatively small
- Telephone Number
- Fax Number
- E-mail Address
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary
- Account Number
- Certificate/License Number
- Any Vehicle or Device Serial Number
- Web URL
- Internet Protocol (IP) Address
- Finger or Voice Prints
- Photographic Images
- Any Other Unique Indentifying Number, Characteristic, or Code (whether generally available in the public realm or not)

## Sharing of Information with Family and Friends Involved in the Patient's Care by Physicians

Generally you may share information directly relevant to the person's involvement with the patient's care or for payment related to care under the following circumstances:

If the patient is present or otherwise available prior to the disclosure, you must:

- Obtain the patient's agreement **or**
- Provide the patient an opportunity to object, and they do not **or**
- Using professional judgment, reasonably infer from circumstances that the patient does not object

If the patient is not present, or is incapacitated, or in an emergency situation, you may provide:

- The information directly relevant to family/friend's involvement in the patient's care, if you determine it is in the patient's best interest

MCMH must take ***reasonable*** steps to make sure PHI is kept private. Incidental disclosures happen when reasonable safeguards have been taken to protect a patient's information and a visitor or another patient happens to hear or see the PHI that you are using. You will not be liable for incidental disclosures, provided you are taking reasonable precautions.

- Dispose of PHI properly by shredding or placing in a locked shredding bin
- Remove patient labels from lab coats or scrub jackets before going outside
- When accessing PHI on a computer, be aware of anyone nearby and do not allow them to view your computer screen
- Log off or lock your computer prior to stepping away from It
- Do not leave PHI on unattended desks, computer terminals, fax machines, or copiers

## Safeguards (cont)

- If you happen to notice PHI that is left out, do not read it – close it or put it away
- PHI used in public areas should be placed face down on the desk/counter or placed in a folder
- After business hours or when not in use, PHI should be supervised or kept in a locked location
- Avoid discussing PHI in public areas such as cafeterias and hallways

Security (protecting the system and the information it contains) includes

*protecting against unauthorized access from outside and misuse from within*

- hardware and software (Physical Computer Systems)
- personnel policies
- information practice policies
- develop disaster/intrusion/response and recovery plans
- designate security responsibilities
- develop protocols regarding activities and security at personnel and work station level
- Safeguards from fire, natural and environmental hazards and intrusions

# General Security Awareness

## Two Types of Security in HIPAA

Building\Physical Security

- Building\Work Area Access
- Locks and Keys
- Badges\ID
- Security Officer
- Printers\Copy\Fax Machines

Computer\Electronic Security

- Computers
- Location of PCs
- Passwords\Log On
- E-mail
- Faxes

# General Security Awareness

Computer\Electronic Security

- Computers
- Location of PCs
- Passwords\Log On
- E-mail
- Faxes
- Be aware of potential harm
- Follow the e-mail policy
- Don’t download non-MCMH approved programs
- Don’t go to web sites that are not work related
- Report unknown or suspicious e-mail, attachments

# Password Security

What is Password Security?

Don’t tell anyone your password.

Don’t tape your password to your monitor, keep it in a secure place!

Change password if others know it

Enter your password in private

# Guidelines for good passwords

## **Don’t**

Choose a password that can be found in a dictionary

Choose a password that uses public information such as SSN, Credit Card or ATM #, Birthday, date, etc.

Reuse old passwords or any variation

Use user id or any variation

# Guidelines for good passwords

## **Do**

Use an easy to remember sentence

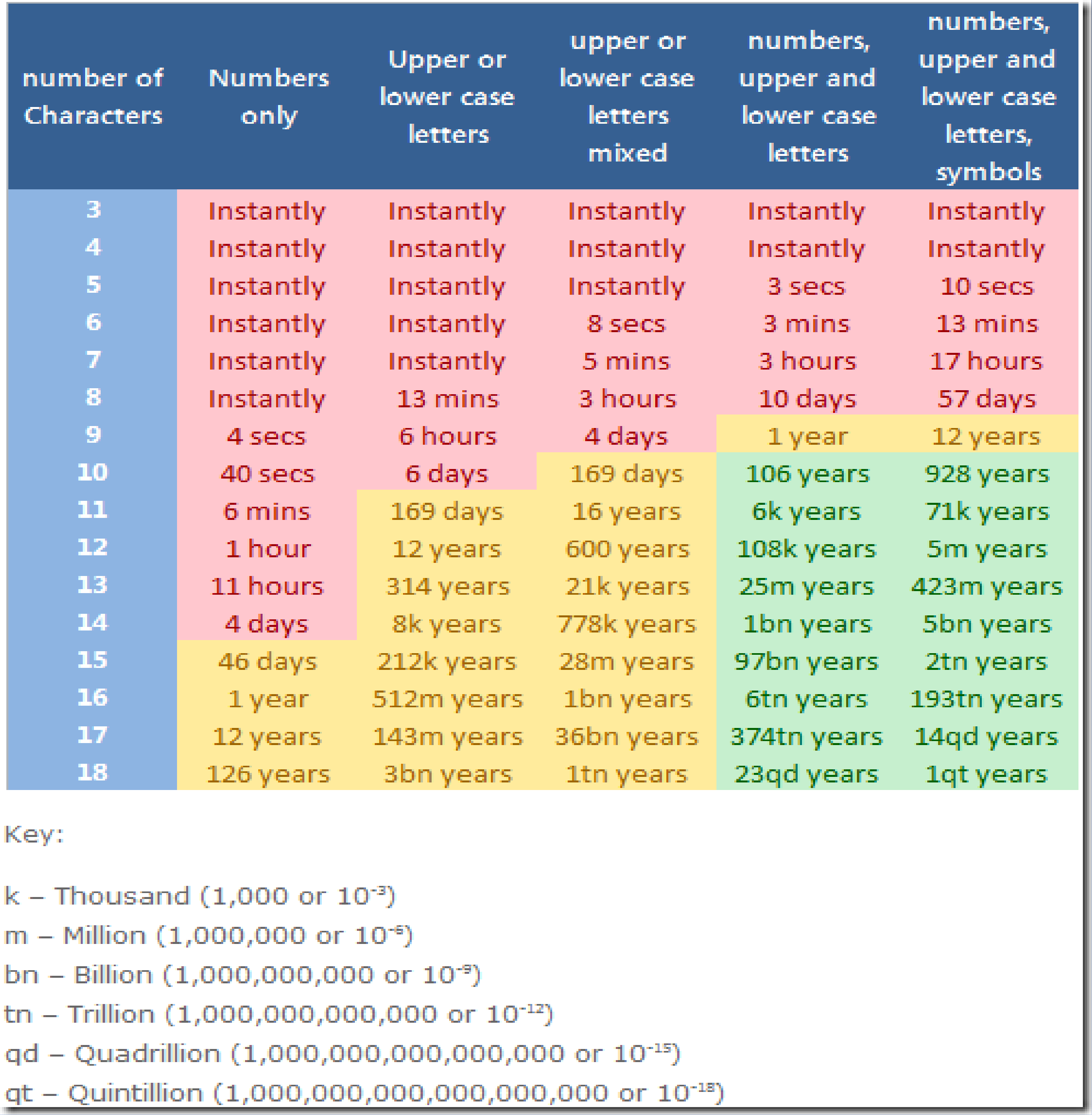
Eight or more characters

Use upper and lower case characters, numbers and a special character (!@$?)

Change to a completely new password each time

Memorize your password

# How long would it take a hacker to crack your password?



| number of Characters | Numbers only | Upper or lower case letters | upper or lower case letters mixed | numbers, upper and lower case letters | numbers, upper and lower case letters, symbols |
|---|---|---|---|---|---|
| 3 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | 3 secs | 10 secs |
| 6 | Instantly | Instantly | 8 secs | 3 mins | 13 mins |
| 7 | Instantly | Instantly | 5 mins | 3 hours | 17 hours |
| 8 | Instantly | 13 mins | 3 hours | 10 days | 57 days |
| 9 | 4 secs | 6 hours | 4 days | 1 year | 12 years |
| 10 | 40 secs | 6 days | 169 days | 106 years | 928 years |
| 11 | 6 mins | 169 days | 16 years | 6k years | 71k years |
| 12 | 1 hour | 12 years | 600 years | 108k years | 5m years |
| 13 | 11 hours | 314 years | 21k years | 25m years | 423m years |
| 14 | 4 days | 8k years | 778k years | 1bn years | 5bn years |
| 15 | 46 days | 212k years | 28m years | 97bn years | 2tn years |
| 16 | 1 year | 512m years | 1bn years | 6tn years | 193tn years |
| 17 | 12 years | 143m years | 36bn years | 374tn years | 14qd years |
| 18 | 126 years | 3bn years | 1tn years | 23qd years | 1qt years |

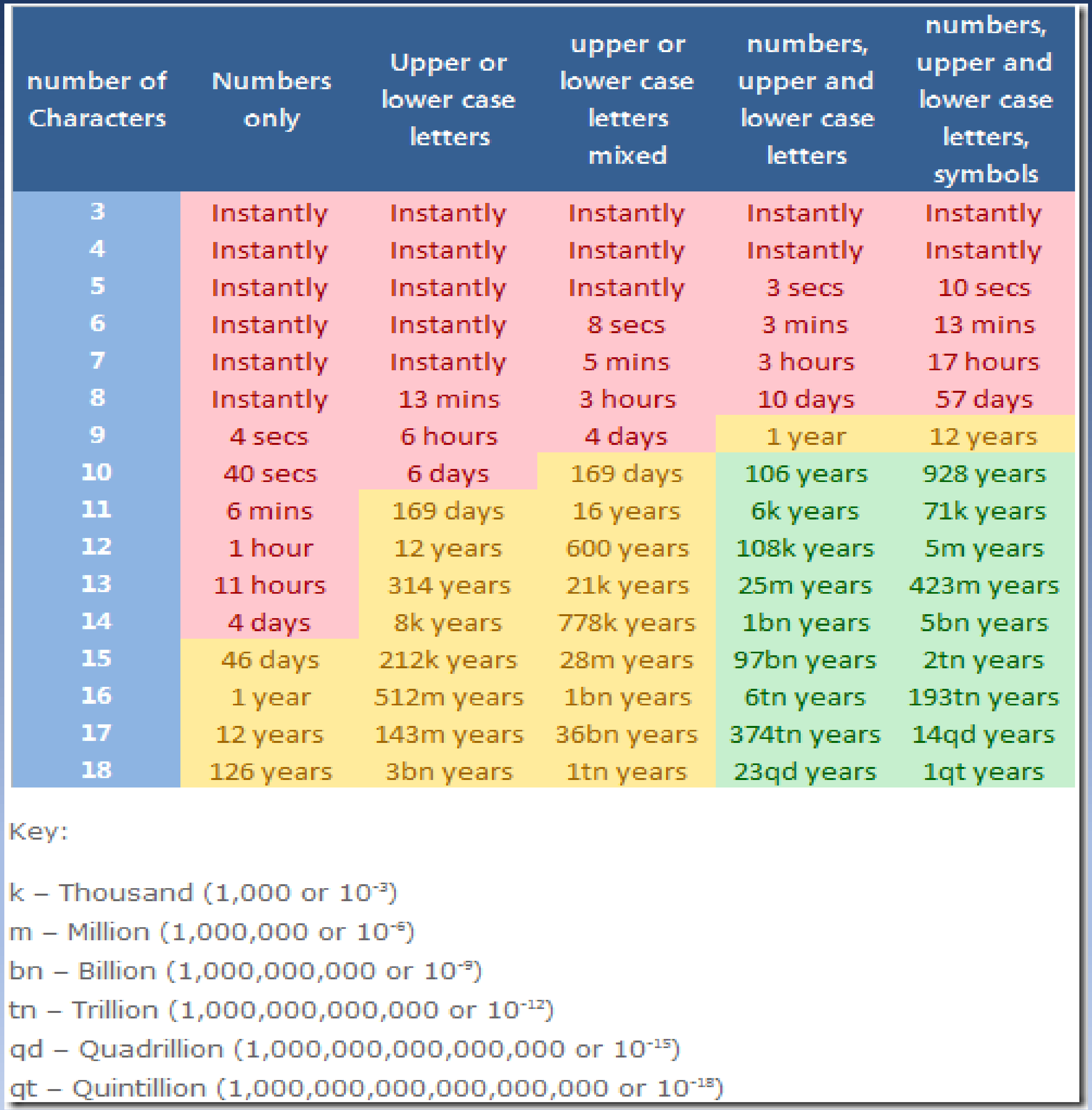
Key:

k – Thousand (1,000 or $10^{-3}$)
m – Million (1,000,000 or $10^{-6}$)
bn – Billion (1,000,000,000 or $10^{-9}$)
tn – Trillion (1,000,000,000,000 or $10^{-12}$)
qd – Quadrillion (1,000,000,000,000,000 or $10^{-15}$)
qt – Quintillion (1,000,000,000,000,000,000 or $10^{-18}$)

Examples of good passwords that are easy to remember:

**Mary is 15!**
Will take the hacker 71,000 years to crack it.

**I have 2 cats!**
Will take the hacker 5 billions years.



| number of Characters | Numbers only | Upper or lower case letters | upper or lower case letters mixed | numbers, upper and lower case letters | numbers, upper and lower case letters, symbols |
|---|---|---|---|---|---|
| 3 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | 3 secs | 10 secs |
| 6 | Instantly | Instantly | 8 secs | 3 mins | 13 mins |
| 7 | Instantly | Instantly | 5 mins | 3 hours | 17 hours |
| 8 | Instantly | 13 mins | 3 hours | 10 days | 57 days |
| 9 | 4 secs | 6 hours | 4 days | 1 year | 12 years |
| 10 | 40 secs | 6 days | 169 days | 106 years | 928 years |
| 11 | 6 mins | 169 days | 16 years | 6k years | 71k years |
| 12 | 1 hour | 12 years | 600 years | 108k years | 5m years |
| 13 | 11 hours | 314 years | 21k years | 25m years | 423m years |
| 14 | 4 days | 8k years | 778k years | 1bn years | 5bn years |
| 15 | 46 days | 212k years | 28m years | 97bn years | 2tn years |
| 16 | 1 year | 512m years | 1bn years | 6tn years | 193tn years |
| 17 | 12 years | 143m years | 36bn years | 374tn years | 14qd years |
| 18 | 126 years | 3bn years | 1tn years | 23qd years | 1qt years |

Key:

k – Thousand (1,000 or $10^{-3}$)
m – Million (1,000,000 or $10^{-6}$)
bn – Billion (1,000,000,000 or $10^{-9}$)
tn – Trillion (1,000,000,000,000 or $10^{-12}$)
qd – Quadrillion (1,000,000,000,000,000 or $10^{-15}$)
qt – Quintillion (1,000,000,000,000,000,000 or $10^{-18}$)

## Communicate Quietly

- Make it a habit – always lower your voice when discussing patient information
- Try to discuss patient care privately
- Stop the conversation if someone walks up while giving report or rounding
- Pull curtains between beds in semi-private rooms
- Escort patient/family out of public hearing range

## Use and Disclosure

**USE** is sharing of protected health information (PHI) within the MCMH network
**DISCLOSURE** is releasing or providing access to PHI to anyone outside of MCMH

Generally, you may use and disclose PHI for treatment, payment, and healthcare operations **(TPO)** of our organization WITHOUT patient authorization
If the requestor is not known to you, VERIFY their identity and authority before providing PHI
**TPO**
**Treatment** – Provision of healthcare by healthcare providers including coordination of care and referrals to other providers
**Payment** – Activities related to reimbursement and premiums such as billing, utilization review, and eligibility determinations
**Operations** – Examples are: training programs, accreditation, credentialing, quality improvement activities, case management, and business planning

## Use and Disclosure

Limited PHI may also be used or disclosed without patient authorization when *required* by law

Examples of disclosures required by law:

- Births and deaths
- Deaths from suspicious circumstances
- Disease reporting to the Department of Health for specific diseases identified by statute
- Sudden Infant Death Syndrome (SIDS)
- Child abuse or neglect
- Abuse of the elderly, endangered, or impaired adult

  **NOTE**: Reporting of abuse of an individual who does not fall into these categories is *<u>not allowed</u>* without authorization
- Intentional infliction of knife or gunshot wounds
- Reporting to registries, such as cancer or organ transplantation
- Disclosure to regulatory agencies such as CMS, FDA, licensing boards, etc.

Any access, use, or disclosure of confidential information outside of your job duties is prohibited

Never share your password with anyone (this includes people working with you, for you, or under you or to IT personnel) and do not leave it accessible to anyone

Do not access information except to meet needs specific to your job

**Signing the MCMH Confidentiality Agreement is a condition of employment at MCMH**

**Breach of confidentiality is a terminable offense**

## Faxing

- Confidential data should be faxed only when mail will not suffice
- Faxes containing PHI and other confidential information must have an official MCMH fax cover sheet
- Reconfirm recipient’s fax number before transmitting.  Use preset fax numbers when possible
- Confirm receipt of fax
- Notify your supervisor/HIPAA Office immediately if a fax is sent in error

## Printed PHI

Do not leave PHI “lying around” where others can see it

Do not put PHI, including patient stickers and medication labels, in the regular trash.  Shred or place in the locked shred bins

Obliterate patient information on IV bags or cover with white labels before placing in the regular trash

When retrieving information from the printer and mailing/faxing information, check every page to make sure it is the correct patient

## Electronic PHI

Be aware of your computer screen

- Position your monitor so the screen cannot easily be seen by anyone passing by
- Minimize the screen if someone walks up
- Log off or lock your computer prior to stepping away from it
- Encrypt any e-mail containing PHI sent over the internet
- Remember that all e-mails are the property of MCMH

**Passwords**

- Always maintain and use passwords in a secure and confidential manner
- Never share your password or use someone else’s sign on information
- If you are asked to sign on using someone else’s information, refuse to do so and report them

**Violations**

→ Violations of HIPAA are taken seriously and can result in dismissal, fines, and/or imprisonment

→ It can happen to you if you inappropriately access a patient's record that is not part of your job duties

→ It can also happen to you if you disclose PHI to anyone outside of MCMH

**Accidental Disclosure**

Mistakes happen… If you disclose private data in error to an unauthorized person or if you breach the security of private data

- Acknowledge the mistake, and notify your supervisor or HIPAA Office immediately
- Learn from the error – change procedures or practices as needed
- Assist in correcting or recovering from the error ONLY if instructed to do so – do not try to cover it up or "make it right" on your own

## Intentional Disclosure

If you ignore the rules and carelessly or deliberately use or disclose PHI inappropriately, you can expect MCMH disciplinary action, civil liability, and/or criminal charges

All intentional violations, known or suspected, must be reported immediately

- To be investigated and managed
- To be prevented from happening again
- Damages can be kept to a minimum
- To minimize personal risk

# HIPAA Enforcement Requirements

- Strict liability fines up to $1,500,000 per occurrence
- Requirement that we notify AHCA of a “breach” including inappropriate access to a patient’s record

***You can be held personally liable!***

## What Can You Do To Help

- Notify the MCMH HIPAA Office as soon as you suspect a possible breach
- The HIPAA Office will then determine if any actual breach has occurred and take care of the notification process
- Help us keep patient contact information current
- Follow your department’s documentation requirements
- Take steps to prevent breaches from happening in your department
- Never access patient information except as needed to perform your job
- When in doubt it is best to report

**Remember: Be Aware of PHI**

- When papers containing PHI are no longer needed, place them in a locked shred bin
- Be careful not to leave PHI at copy or fax machines, printers, or in conference rooms
- When retrieving information from the printer and mailing/faxing information, check all pages to make sure it is the correct patient
- Do not take patient charts out of the hospital
- Turn computer screens away from traffic or use privacy screens and be aware of those around you when using PHI on computers
- Log off or lock your computer prior to stepping away. You are responsible for all access under your log-on credentials