HIPAA

Training for Doctors and Staff

Health Insurance Portability and Accountability Act

NACATexas

CRUISING THE FJORDS

NACATexas

MICHELE QUATTLEBAUM

2012, 2013, 2014, 2015,2016, 2017 & 2018

Texas Super Lawyer

- Board Certified Personal Injury Trial Law
  - Texas Board of Legal Specialization
- Tried chiropractic malpractice cases to verdict since ‘82
- Routinely handles board matters
- Seminars/webinars concerning chiropractic malpractice, documentation, Medicare, Ethics, Risk, and HIPAA

MICHELE QUATTLEBAUM

- Sprott, Newsom,
- Quattlebaum & Messenger PC
  2211 Norfolk Suite 1150
  Houston, TX 77098
  713-523-8338
  713-523-9422 FAX
- quattlebaum@sprottnewsom.com

- mqbandit@aol.com

HIPAA

The law known as HIPAA stands for Health Insurance Portability and Accountability Act of 1996. This law was passed to promote more standardization and efficiency in the health care industry.

There are four parts to HIPAA's Administrative Simplification:

1. Electronic Transactions and Code Sets Standards requirements
2. Privacy requirements
3. Security requirements
4. National Identifier requirements

HIPAA APPLIES TO ALL FORMS OF PHI

- Whether paper or electronic there are privacy and security standards.
- THIS IS NOT LIMITED TO MEDICARE OR FEDERAL FUNDED INSURANCE
- This is ALL PATIENTS, free, cash, insurance, PI, comp, insurance.

THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH)

- HITECH Act widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for non-compliance; and it provides for more enforcement.

WHAT IS PHI….?
PROTECTED HEALTH INFORMATION

- "Individually identifiable health information" is….
  - the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual,
- Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

WHO IS WHO?

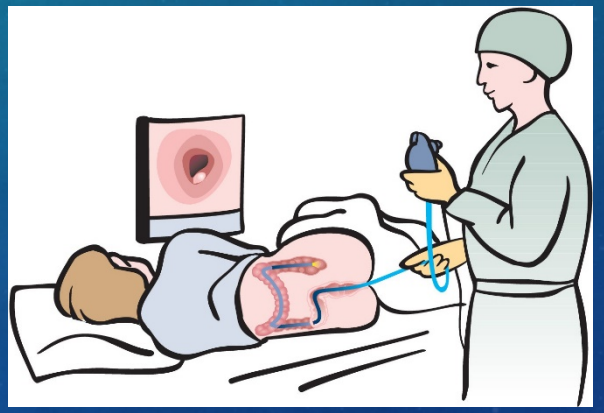
- **HHS:** Department of Health and Human Services
- **OCR:** Office of Civil Rights

AUDITS

- HHS is ramping up its enforcement program. In past when there were complaints, now starting auditing program
- “no immunity” and prosecution is always a possibility
- Penalties can range from civil penalties up to 1.5 million dollars to 10 years in jail for criminal acts
- If notice of audit, you must respond

AUDITS

- A “paper audit” can turn into an on-site audit,



WHAT IS THE SECURITY RULE….??

The HIPAA Security Rule requires implementation of three types of safeguards:

- 1) administrative
- 2) physical, and
- 3) technical

BIGGEST SECURITY RISK

- Is not your electronics
- IT IS YOUR PEOPLE

ADMINISTRATIVE SAFEGUARDS

- Administrative safeguards are administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information.

ADMINISTRATIVE

- Must adopt a written set of privacy procedures
- Designate a Privacy Officer
- Implement all required policies and procedures
- Policies must reference management oversight and organization buy-in to compliance with the documented security controls.

ADMINISTRATIVE

- **Identify which employees will have access to electronic protected health information**
- **Access denied to those who don't need information to complete their job function**
- **Authorization, establishment, modification, and termination.**
- **Training program**
- **If out source to a third party must ensure that their vendors also have framework for HIPAA compliance**

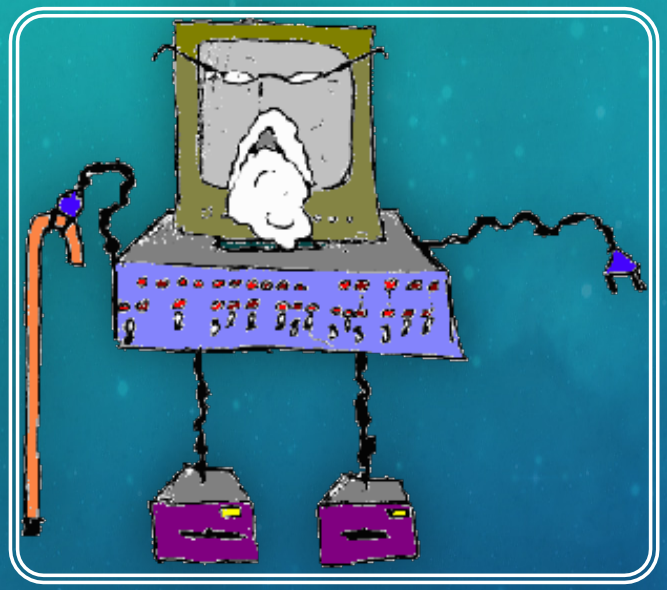
ADMINISTRATIVE

- Contingency plan for responding to emergencies
- Backing up data
- Disaster recovery procedures in place
- Internal audits
  - Routine and event based
  - Policies and procedures for scope and frequency of audit
- Instructions for addressing and responding to security breaches that are identifiable during audit or in normal course of business

PHYSICAL SAFEGUARDS

- **Physical safeguards are physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion**.

PHYSICAL



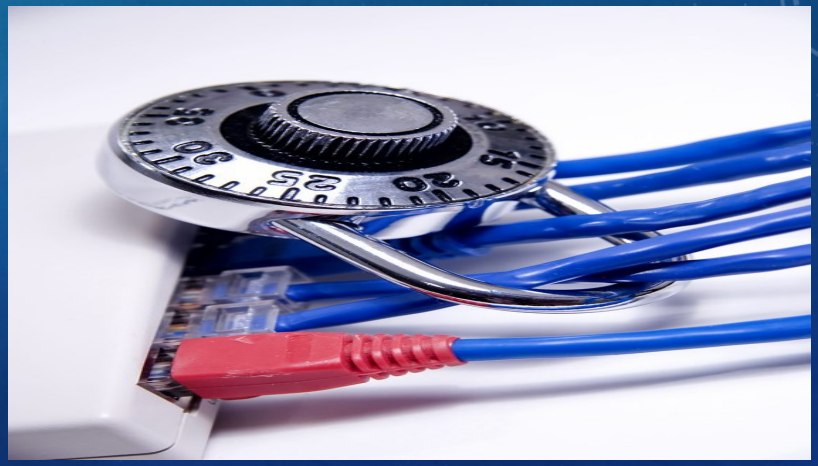
- Controlling physical access to protect against inappropriate access to protected data
- Introduction and removal of hardware and software from the network
- When retire equipment it must be disposed of properly to ensure that PHI is not compromised
- Access to equipment containing PHI should be carefully controlled and monitored

PHYSICAL

- Access to hardware and software must be limited to properly authorized individuals
- Required access controls consist of facility security plans, maintenance reords, and visitor sign-in and escorts.
- Workstations should be removed from high traffic areas
- Monitor screens should not be in direct view of the public
- Contractors or agents, must be fully trained on their physical access responsibilities

TECHNICAL SAFEGUARDS

- Technical safeguards mean technology and the policy and procedures for its use that protect electronic health information and control access to it.



WHAT IS ENCRYPTION

- Encryption software executes an algorithm that is designed to encrypt computer data in such a way that it cannot be recovered without access to the key. Software encryption is a fundamental part of all aspects of modern computer communication and file protection and may include features like file shredding.

- The purpose of encryption is to prevent third parties from recovering the original information. This is particularly important for sensitive data like credit card numbers.

WORD OF ADVICE FROM HHS

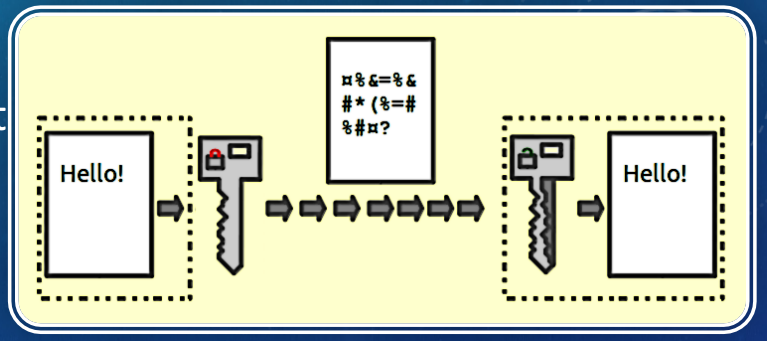
- **Encrypt**
- **Encrypt**
- **Encrypt**

TECHNICAL

- Information systems housing PHI must be protected from intrusion
- When information flowing over open networks, some form of encryption must be utilized. If closed systems , exist access controls are considered sufficient and encryption is optional.
- Each covered entity is responsible for its own data

TECHNICAL

- To insure data corroboration, use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity
- Covered entities must authenticate with whom they communicate
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance



TECHNICAL

- Information technology documentation should also include a written record of all configuration settings on the components of the network (because they are always changing)

TECHNICAL/PHYSICAL

- Laptops/PCs must be secured when not in use
- Do not go to lunch, leaving computer signed on
- Do not give your passwords out

RISK ANALYSIS

- DOCUMENTED RISK ANALYSIS AND RISK MANAGEMENT PROGRAMS ARE REQUIRED. COVERED ENTITIES MUST CAREFULLY CONSIDER THE RISKS OF THEIR OPERATIONS AS THEY IMPLEMENT SYSTEMS TO COMPLY WITH THE ACT.
- This is a minimal standard

PRIVACY SAFEGUARDS

- Protect your Laptop, PDA etc. as well as you do your paper records
- Password protect
- Disposal of hard drives
- Copiers
- Do not share your electronics with family members or friends

PRIVACY SAFEGUARDS

- Remember that a spouse must have an authorization to obtain records
- Kids turning 18
- Can not discuss care with attorney without consent
- Do not share records with anyone for any reason without BAA or authorization without patient authorization

ARE THESE VIOLATIONS ?

- Talking to the spouse about the other spouse's treatment
- Faxing a MRI report to the patient
- Telling your spouse that JJ Watt came to the office with a strained groin muscle today
- Putting medical condition on Back to Work Slip
- Asking a patient at Kroger how their back pain is, when another customer can hear?

VIOLATIONS??

- Having a patient fill out an intake form and after you input it you throw it in the trash
- Leaving a patient file on the ledge in the clinic
- Using a thumb drive that is not encrypted
- Faxing a report from Kinkos
- Billing for a ultrasound when one wasn't performed
- ***UPCODING***

Date	Organization	Fine Total	Link to OCR Settlement
February 1, 2018	Fresenius Medical Care North America (FMCNA)	$3,500,000	Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules
February 13, 2018	Filefax, Inc.	$100,000	Consequences for HIPAA violations don't stop when a business closes

Date	Organization	Fine Total	Link to OCR Settlement
January 9, 2017	Presence Health	$475,000	First HIPAA enforcement action for lack of timely breach notification settles for $475,000
January 18, 2017	MAPFRE	$2,200,000	HIPAA settlement demonstrates importance of implementing safeguards for ePHI
February 1, 2017	Children's Medical Center of Dallas	$3,200,000	Lack of timely action risks security and costs money
February 16, 2017	Memorial Healthcare Systems	$5,500,000	$5.5 million HIPAA settlement shines light on the importance of audit controls
April 12, 2017	Metro Community Provider Network (MCPN)	$400,000	Overlooking risks leads to breach, $400,000 settlement
April 20, 2017	The Center for Children's Digestive Health (CCDH)	$31,000	No Business Associate Agreement? $31K Mistake
April 24, 2017	CardioNet	$2,500,000	$2.5 million settlement shows that not understanding HIPAA requirements creates risk
May 10, 2017	Memorial Hermann Health System (MHHS)	$2,400,000	Texas health system settles potential HIPAA violations for disclosing patient information
May 23, 2017	St. Luke's Roosevelt Hospital System Inc.	$387,200	Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k
December 18, 2017	21st Century Oncology	$2,300,000	$2.3 Millon Levied for Multiple HIPAA Violations at NY-Based Provider
	2017 TOTAL:	**$19,393,200**	

TESTIMONIALS

- MUST get written permission to post a testimonial
- If doing it electronically must state that are
- Keep all permissions to use testimonials for 2 years

DO NOT POST…….

- ‘guess who came in to our office today?”

PHOTOS/YOUTUBE

- Photos with celebrity patients.
- GET WRITTEN PERMISSION TO DO SO
- YOUTUBE
- GET WRITTEN PERMISSION TO POST IT ONLINE.

NACATexas

HIPAA POLICIES IN A NUTSHELL

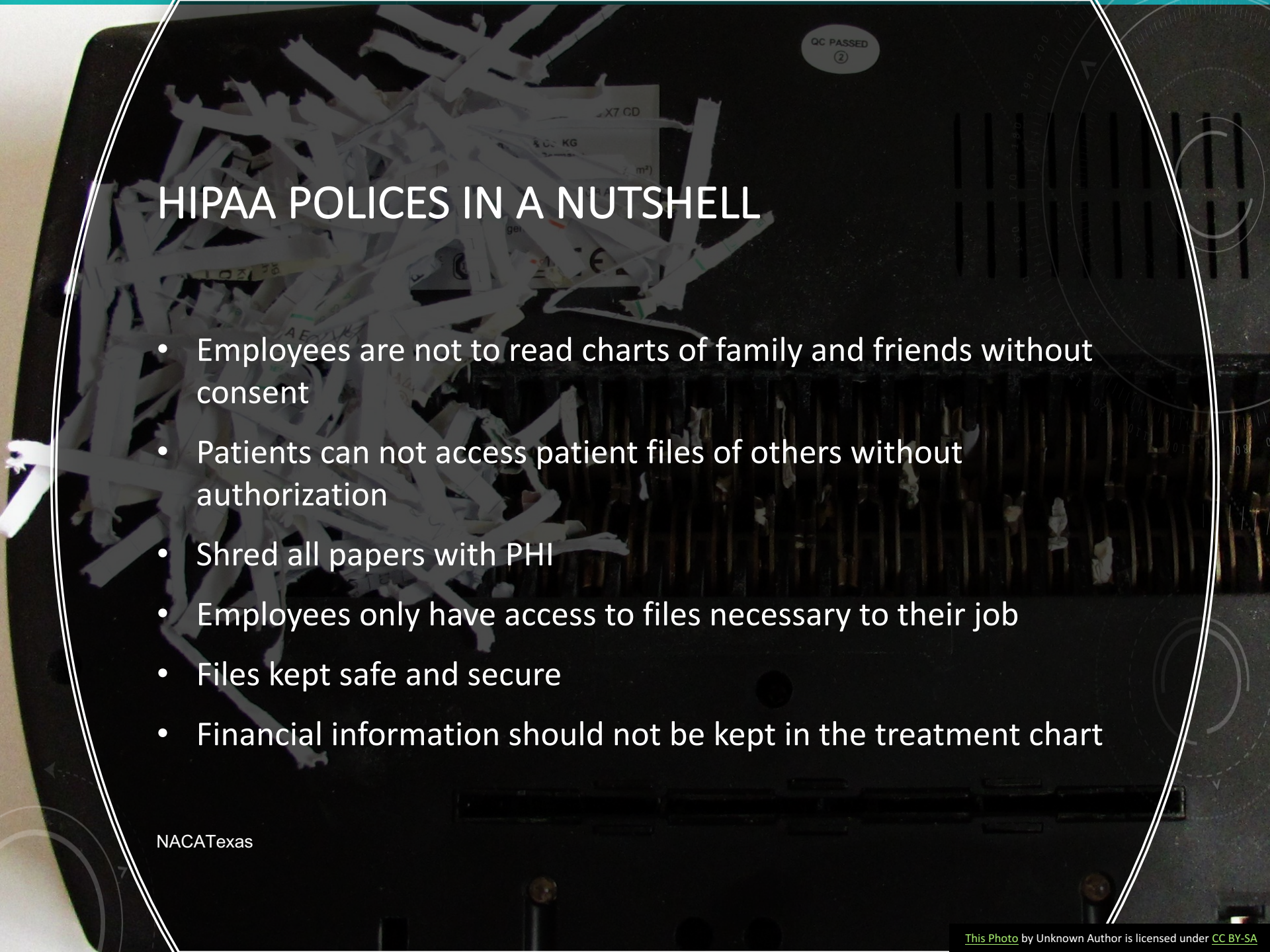
- Patients should not be called by their full name
- Sign in sheets, should NOT list condition, address or any other PHI
- Patients offered privacy notice to take home
- Patients should sign acknowledgement that they received privacy notice

HIPAA POLICIES IN A NUTSHELL

- Privacy Notices must be “posted” in waiting room
- Can put copies in the waiting area
- Do not discuss treatment or payment in the waiting room or within hearing of other patients
- Charts and PHI kept at reception desk in a manner that patient information can not be seen (charts, checks, claims, appointment books)

HIPAA POLICIES IN A NUTSHELL

- Patients can’t see computer screen
- Privacy screens on computers
- Staff on phone can’t be heard by other patients
- Talking in hallways can not be overheard



HIPAA POLICES IN A NUTSHELL

- Employees are not to read charts of family and friends without consent
- Patients can not access patient files of others without authorization
- Shred all papers with PHI
- Employees only have access to files necessary to their job
- Files kept safe and secure
- Financial information should not be kept in the treatment chart

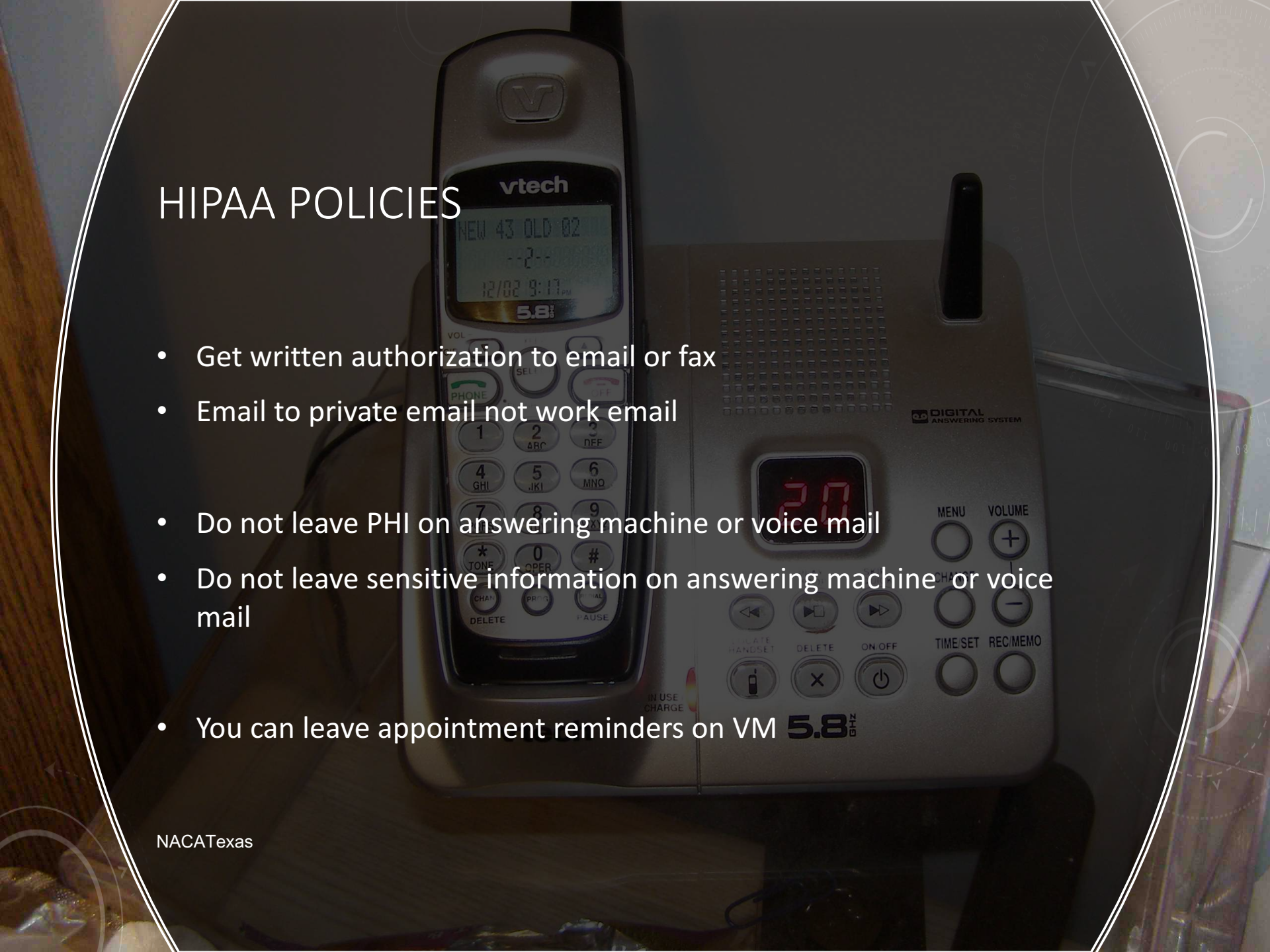
HIPAA POLICIES IN A NUTSHELL

- All discarded information must be shredded
- Records should never be unsecured, unattended or visible to the public
- If charts in a chart rack, they must be positioned so not to identify the patient to passer-bys

HIPAA POLICIES

- Faxing to another doctor does not require patient authorization but only send information necessary for consultation
- Get written authorization to fax
- Emails to patients containing PHI must be confirmed before sending

HIPAA POLICIES



- Get written authorization to email or fax
- Email to private email not work email

- Do not leave PHI on answering machine or voice mail
- Do not leave sensitive information on answering machine or voice mail

- You can leave appointment reminders on VM

HIPAA POLICIES

- Unless requested by the patient, back to work slips should not divulge the illness, disease or reason patient is out of work

POLICIES

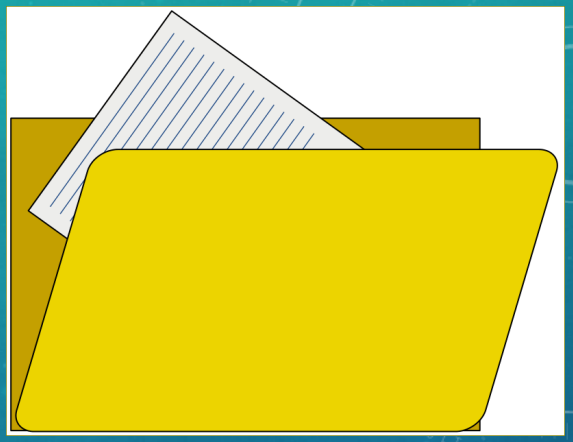
- Do not leave materials on the copiers, fax unattended
- **Do not go to a public location to transmit PHI**
- **Do not copy patient files in a public location**
- **Use encrypted thumb drives**

BILLING FOR SERVICES NOT RENDERED

- therapies, procedures etc
- UPCODING
- MISCODING

- HIPAA VIOLATION
  - Intentional use of PHI for financial gain
  - $250,000
  - 10 years in jail

OFFICE CHARTS



- Do not leave them out at front desk
- Do not leave them where people signing in can read them,

PAPER PHI- PROTECTION MECHANISMS

- Confidential recycle bins
- Secure fax machines
- Clean desk policy
- Secure printer
- Prohibition against the use of post it notes to record PHI or passwords

PASSWORDS

- Do not save passwords
- Do not store password near your computer
- Change password every 6 weeks or when necessary
- Minimum of 8 digit password
  - Capital and lowercase
  - Numbers
  - Symbols
  - If PDA only have potential for 4 digits, change often

WHEN AN EMPLOYEE LEAVES

- When an employee leaves
- Passwords changed
- Locks changed
- Exit interview should include privacy matters and have **them once again sign that they understand that the confidentiality requirements still exist**

SAFEGUARD THE OFFICE

IS YOUR OFFICE SAFE? SECURE?

- Patient records in a secure area?
- Names on charts protected?
- Screens on computers at front desk?
- Is the information at front desk protected?
- Can patients hear calls at front desk?
- Computers with rapid time out? password protected?
- Laptops secured?
- Computers locked?

IS YOUR OFFICE SECURE? SAFE?

- Security cams at front desk
- Security locks on doors?
- Security alarms?
- Limited access to keys?
- Does your sign in sheet contain health information?
- Phone messages in protected area?
- Charts not left out with identifiable information?

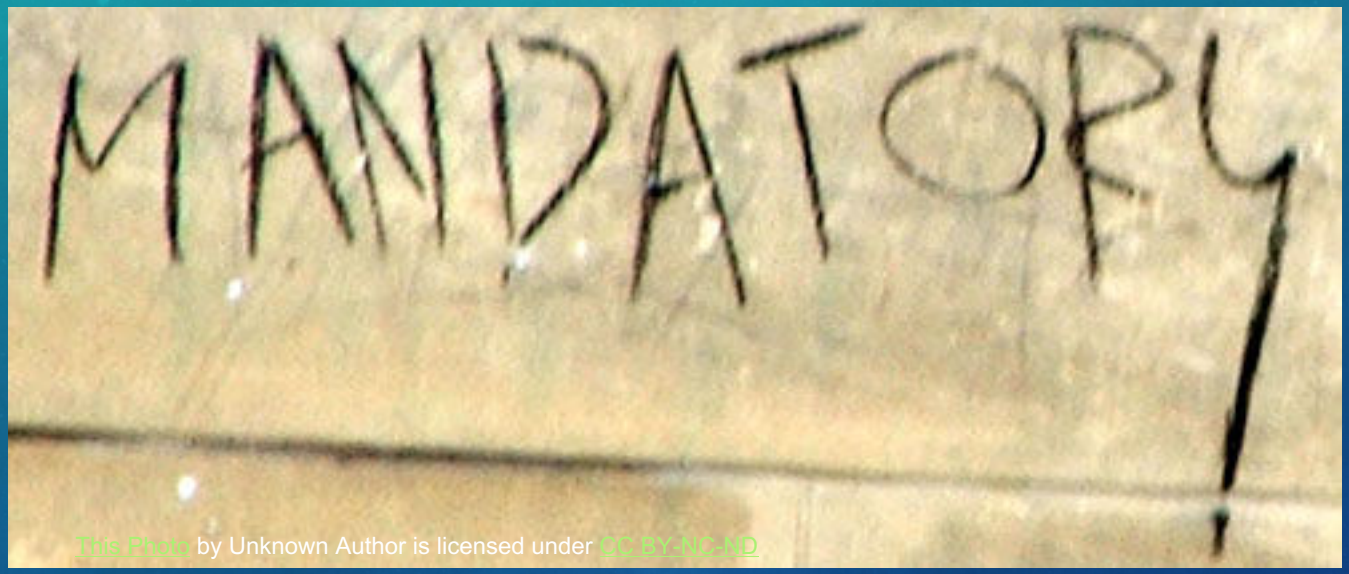
IS YOUR OFFICE SAFE? SECURE?

- Are charts left in treatment rooms?
- X-rays taken off the view boxes?
- Is patient information being discussed in common areas?
- Patient Rights forms accessible upon request?

HIPAA MANUAL

NACATexas

HIPAA MANUAL

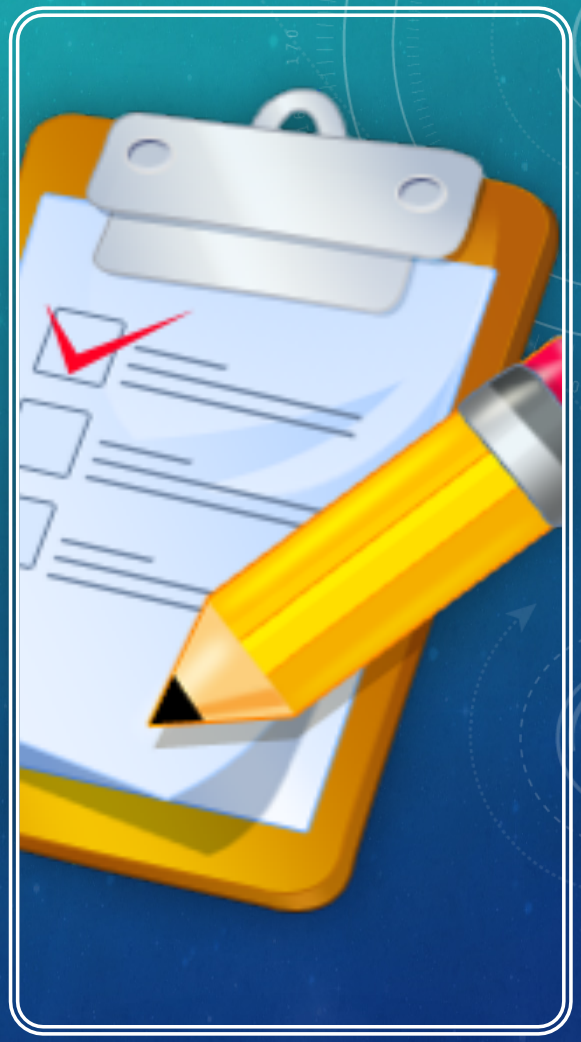


HIPAA MANUAL

- Must list the HIPAA Rules and Violations
- You need to customize it to your office
- Forms
- All your office reads it
- Staff Member discussion
- Can be part of your staff training
- Incidents
- Disclosures
- Training materials
- But must be personalized

PRIVACY PRACTICES NOTICE

- Fill in the Blanks
- Display in the Reception area
- Make Extra Copies Available to Patients
- Put on Your Website
- Update as Needed

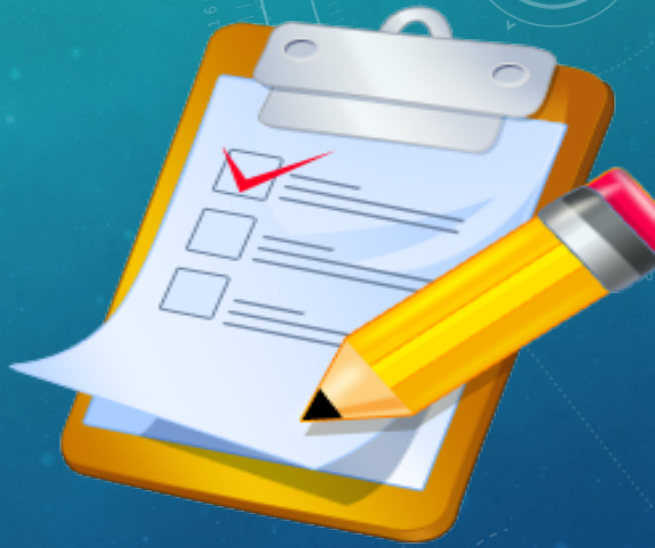


NACATexas

IF YOU TRANSMIT ELECTRONICALLY

- You must put on website and display in office
- ***"this office transmits patient protected health information electronically"***

ACKNOWLEDGEMENT OF PRIVACY PRACTICES



- Fill in Blanks
- Make Copies for Front Desk
- Direct all Patients to the Notice in the reception area
- Have all Patients Sign the Acknowledgement
- Afford the Patient of a Copy if Requested
- Put in Patient's File

BUSINESS ASSOCIATES AGREEMENT

- Fill in Blanks
- Acquire Business Associate's Signature
- Maintain a Business Associate File
- Document in Patient's File When PHI is released to Business Associate
- Update annually
- Subcontractor

WHO ARE BUSINESS ASSOCIATES…?

- A CPA firm
- An attorney
- A consultant that performs utilization reviews
- A health care clearinghouse
- An independent medical transcriptionist
- Outside billing company
- IT company

HITECH AND BUSINESS ASSOCIATES

- Under the HITECH Act, Business Associates are now directly "on the compliance hook" since they are required to comply with the safeguards contained in the HIPAA Security Rule (SR).

BUSINESS ASSOCIATES

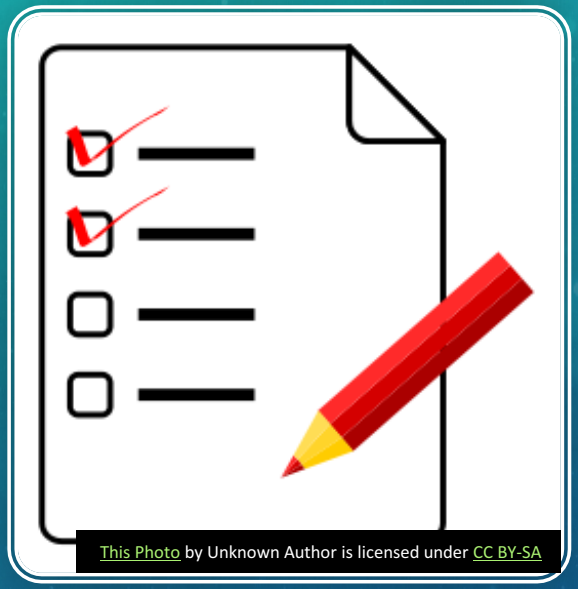
- You do not have to personally train the BAA
- BUT you need to confirm that they train their staff
- Confirm they understand the HIPAA rules
- For instance, ask who their compliance officer is?

INCIDENTAL USES AND DISCLOSURES

- Sign in sheets
- Using a patient's name in the clinic
- Seeing a patient's name on a file

The Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual's privacy.

ACCOUNTING OF DISCLOSURES



- Accounting of Disclosures
- Make Copies
- Complete When PHI is Disclosed as Directed
- Maintain in Patient's File

MISCELLANEOUS FORMS

- Miscellaneous Forms
- Make Copies
- Complete When Necessary
- Maintain in Patient's File

  - Request to Inspect or Copy Protected Health Information
  - Approval of Request to Inspect or Copy Protected Health Information
  - Denial of Request to Inspect or Copy Protected Health Information
  - Request to Amend Protected Health Information
  - Decision to Approve or Deny Request to Amend Protected Health Information
  - Release of Protected Health Information

EMPLOYEE CONFIDENTIALITY AGREEMENT AND UNDERSTANDING

I,_____, whose duties are that of a _____ , understand that I have the same privacy, security and confidentiality requirements as the doctor with regard to Patient care and treatment. I have an obligation and duty to protect and safeguard all patient protected health information from disclosure, whether intentional or inadvertent. I have an obligation to produce all information properly requested to the patient. I agree to keep all patient health and personal information protected from disclosure and follow all federal and state laws regarding patient privacy and confidentiality.

I have been trained in HIPAA and acknowledge that I have an obligation to understand and follow that training in my employment and after the date I might be terminated. The obligation of confidentiality of patient's protected health information extends past my employment with the clinic.

_____

Employee Signature

_____

Printed Employee Name

_____

Employer Signature

_____

DATE

Authorization to Fax/Email

I recognize that communication done electronically does not have any guarantee of privacy, however due to convenience and timing, communications might be necessary by electronic means of fax and email. I consent to communication specified below. Should I wish to withdraw the consent below I will notify the doctor/clinic in writing of the withdrawal of consent.

I, _____do hereby authorize _____ to communicate with me via fax at the following fax number_____.

_____ _____ Patient Signature

_____Patient Name

_____Date

****

I, _____do hereby authorize _____to communicate with me via email at the following email address_____.

_____ _____ Patient Signature

_____Patient Name

_____Date

NOTIFICATION OF BREACH

- The HITECH Act now imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." These notification requirements are similar to many state data breach laws related to personally identifiable financial information (e.g. banking and credit card data). HHS is required to define what "unsecured PHI" means within 60 days of enactment. If it fails to do so then the HITECH definition will control. Under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI.“

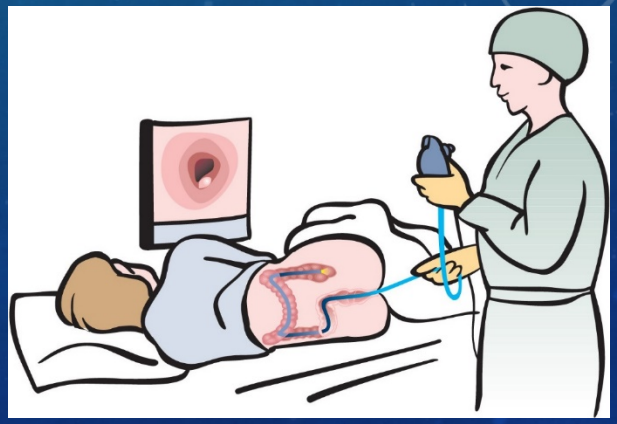
- In general, the Act requires that patients be notified of any unsecured breach. If a breach impacts 500 patients or more then HHS must also be notified. Notification will trigger posting the breaching entity's name on HHS' website. Under certain conditions local media will also need to be notified. Furthermore, notification is triggered whether the unsecured breach occurred externally or internally. The notification provision is yet another example of the weight privacy and security concerns are given under the Act.

IF THERE IS A BREACH YOU MUST

- Show you notified the patient of the breach
- Show the remedial measures you did to correct the breach and for it not to happen again
- Breach notification with the Secretary of the US Department of Health and Human Services if over 500 patients involved of unsecured data

Will have to produce to DHHS a copy of her HIPAA policies and procedures

DHHS will investigate.



IF BREACH OF SECURED DATA

- You do not have to report to HHS within 60 days of breach
- But must notify HHS within 60 days of the end of calendar year notify them of secured data breach

- Yeah, this sucks!!

IF THERE IS A BREACH

- If there are 10 patients you do not know their current addresses, you must post on website, or do a press release
- If there are 500 patients involved you notify HHS
- You must remediate
- Remediation is HUGE in reducing penalties
- Cant put head in sand

INSURANCE

- Insurance available for data breach, data compromise and cyber liability.
- Various prices

- But the cost of breach can bee $200 per patient
- (i.e. 3000 patients could cost you $600,000

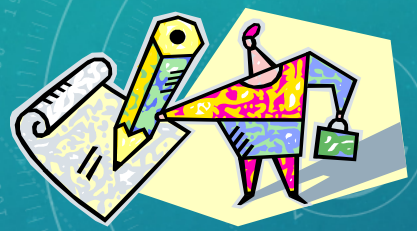
INSURANCE

- On your malpractice policy there should be an attorney fees provision rider.
- 5000 to 30,000 for attorney fees
- Will cover HIPAA investigation and response to OCR
- Not your costs for the data breach.

EXCEPTIONS TO CONFIDENTIALITY

- Court or Administrative Proceeding
  - Brought by patient against Chiropractor
  - A malpractice proceeding
  - Criminal or license revocation where patient is complaining party
  - Debt collection

EXCEPTIONS TO CONFIDENTIALITY



- Written authorization by patient
- Brought by patient to recover monetary damages for physical condition of patient
- Disciplinary action against doctor
- Criminal prosecution in which patient is victim, witness, or defendant

EXCEPTIONS TO CONFIDENTIALITY

Can disclose to medical or law enforcement personnel if the chiropractor determines that a probability of imminent physical injury to the patient, the chiropractor, or others exists or a probability of immediate mental or emotional injury to the patient exists

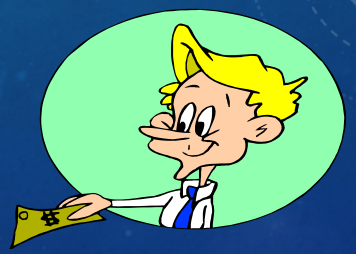
HIPAA PENALTIES

- $100 to $50,000 up to $1,500,000 (after 2-18-09)

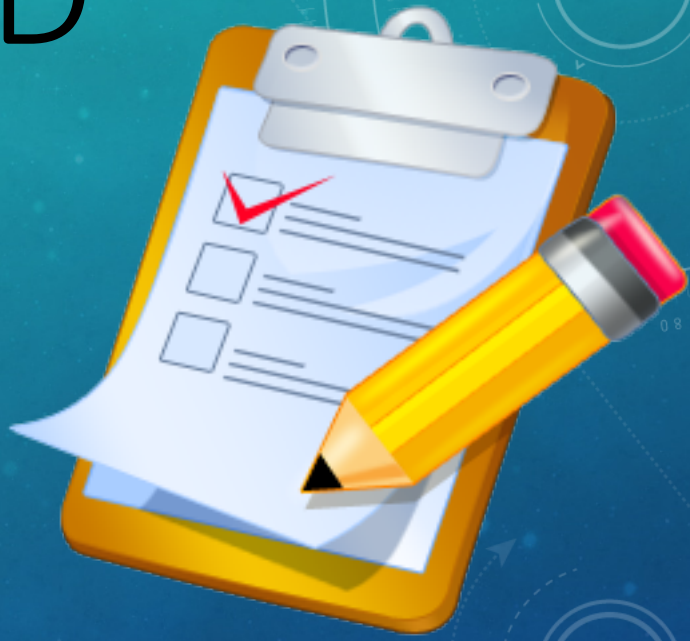
- Under certain circumstances, HHS may not impose civil money penalty such as when a violation is due to reasonable cause, and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of violation

HIPAA PENALTIES

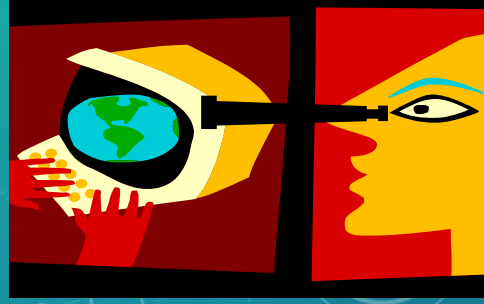
- Knowingly obtains or discloses PHI
  - 1 year imprisonment
- Wrongful conduct involves false pretenses
  - $100,000
  - 5 years imprisonment
- Wrongful conduct involves intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm
  - $250,000
  - 10 years imprisonment



TO GET STARTED



- Select a Privacy Officer
- Safeguard the Office
- Read the Privacy Chapter **(your HIPPA MANUAL)**
- Fill in Blanks
- Distribute to all Staff **(This is training of the staff)**
- Schedule Staff Meeting
- Sign Employee Agreement and File in Employee's Employment File
- Update Training as Needed **(HB 300 – 60 days from hiring then every other year)**



PRIVACY OFFICERS DUTIES

- **General Purpose:** The privacy officer oversees all ongoing activities related to the development and adherence to policies and procedures covering the privacy of; and access to, protected health information in compliance with federal and state laws.

- See the Privacy Officer's Job Description

- Be SAFE
- Be Secure
- Be Compliant