March 07, 2013

OVERVIEW OF HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

Dr. Raghunath Puttaiah

OSHA4Dental Inc.

drputtaiah@gmail.com

Who needs to be trained

- All clinic staff….everyone
- People who handle your patient records
- People who handle your patient financial info
- Your referral end point (dentist, lab, periodontist, oral surgeon….)
- Insurance company you call to get or send patient info
- Covered entities (who are these guys….)
- Discuss…

You may want to educate your dentists

- Covered entities---
- List them out in this discussion
- Talk ,,,,Please Talk….

Topics Covered in this Module

- This course provides an overview of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Privacy of Patient Information
- Security Rules on Patient Information
- Overview of HITECH Act of 2008
- Overview of Texas House Bill 300 amendment

Objectives

- Understand the Implications of HIPAA, HITECH and TX HB 300
- How HITECH Act impacts “Covered Entities” & “Business Associates”
- Understand application of patient privacy during provision of care
  - Patient information confidentiality (Health Info, Financial Info $$$...)
  - Patient’s rights for accessing their health information
  - Determination whether disclosures of PHI are acceptable and protected
- Understand how to protect patient information both digitally and physically using security measures within the clinic and outside
  - Restricted access to information and release on need and specifically to those providing direct care
  - Protection of electronic information within the clinic and outside
  - Prevent identity theft and understand the “Red Flag Rule”
- Understand Texas HB 300 and its amendments

Figuratively speaking.....it is complex

Privacy

Security

Unique Identifier

Transaction and code sets

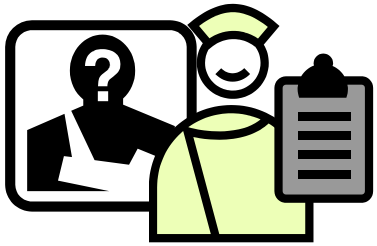
TX HB 300

Enforcement

HIPAA

Information Breach, Costs, Fines*

- **Healthcare Institutions—**
  - Use Mobile Computing (PC, iPad, Tablets, Smart Phones), data transfer devices, email, social media with little or no security systems in place or without security upgrades
  - **Hacker's dream** where they send in viruses, pre-programmed worms, executable files that download information/data sets that can be sold in the **BLACK MARKET**



- **Organization Not Prepared**
  - 61% not confident about PHI location
  - 69% Hospitals have inadequate controls
  - Only 29% felt that PHI is high priority
- **Cost of Breaches**
  - 2009-2011 about 18,000,000 records breached
  - 32% Increase in PHI breaches
  - Annual Cost of Security **$6.5 Billion**
  - **96% Provider** had at least one breach

***Dell PDF**: http://www.secureworks.com/assets/pdf-store/other/infographic.healthcare.pdf

Information Breach, Costs, Fines*

- 81% of clinicians use Mobile Devices to Collect PHI
  - Only 49% have implemented Security Systems on Mobile Devices

Black Market Values

- Value of Credit card = $1-6
- Value of Personal Information (SSN+DOB+Zip Code) = $14-18
- **Value of Health Record = >$50**

- **One unencrypted portable device lost with PHI**
  - Lawsuits = $ 250,000
  - Letters to Clients = $ 319,000
  - Identity Theft Monitoring = $1,000, 000

***Dell PDF**:
http://www.secureworks.com/assets/pdf-store/other/infographic.healthcare.pdf

Information Breach, Costs, Fines*

- Penalties per record = $1,000
- Maximum Penalties = **$ 1,500,0000**

- 21 Million Records in 477 breaches reported to the **"Office of Civil Rights"**

Office for Civil Rights

*Dell PDF: http://www.secureworks.com/assets/pdf-store/other/infographic.healthcare.pdf

Question & Answer

Any other examples from the attendees???? Stories to share

History of HIPAA

Catch as Catch Can

No Standardized Rules on PHI's

1996

HIPAA Introduced

1. Simplify Administrative Process

2. Protect Patient Privacy

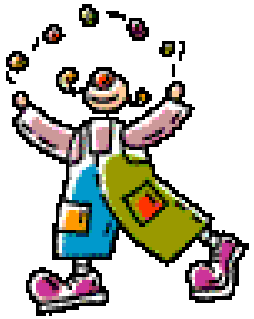
3. Enacted Feb 20th, 2003

Middle Ages

"A star is Born"

2003

History of HIPAA



EHR

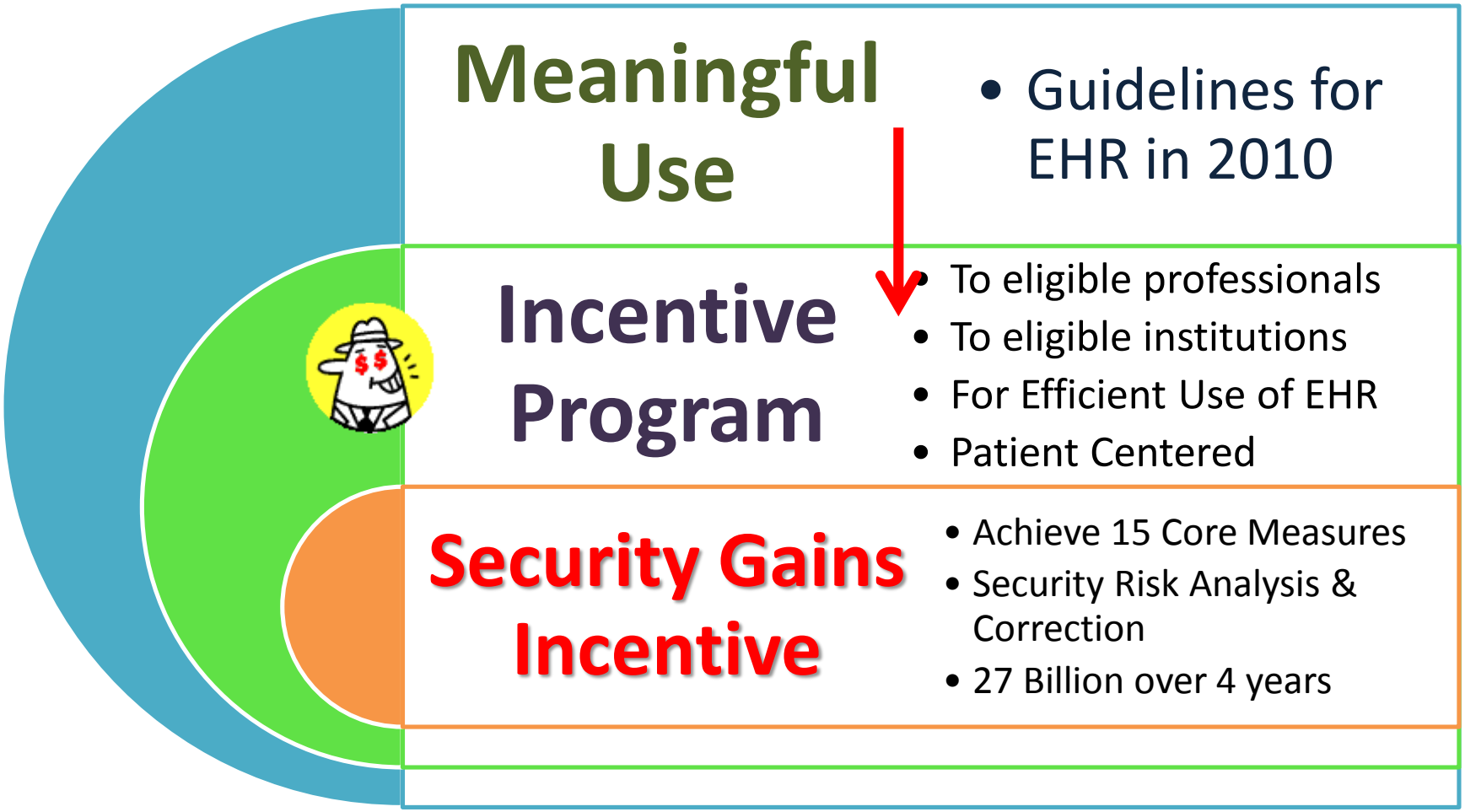
- -Adoption of EHRs
- -Increased Enforcement of HIPAA
- -Increase of Security
- -Cyber Security
- -Increases in Repercussions
- -Standards for EHR Software

ARRA HITECH Act 2009

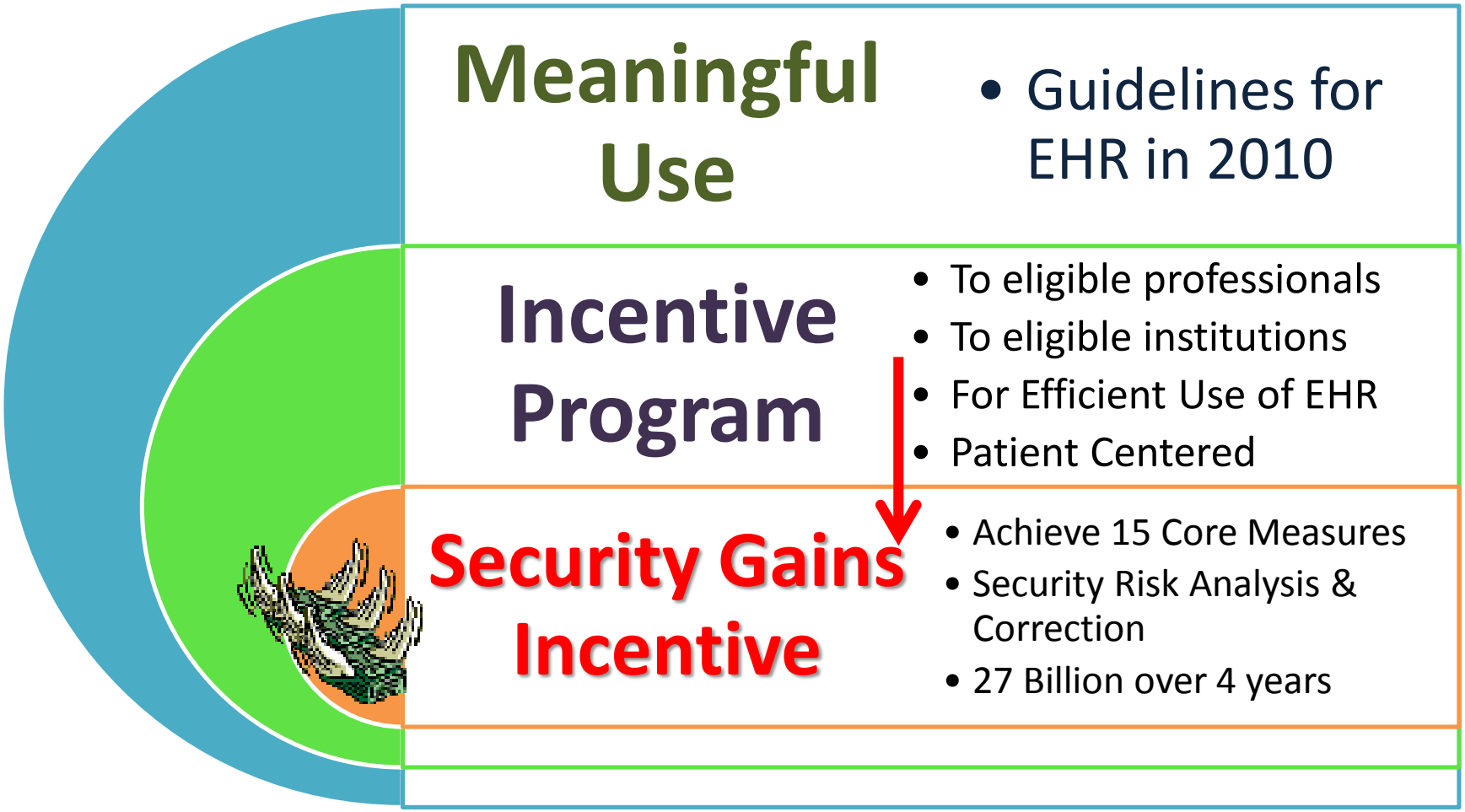
Got Teeth?

- -New Civil Rights Penalties
- -Covered Entities & Business Associates
- -Breach Notification Obligation after September 2009

He-estry of HEEPAA



He-estry of HEEPAA



What is the Basic Use of HIPAA

- This law protects patients' rights with respect to use and misuse of their health and Financial information
- Was to make it easy when patients moved from one insurance plan to another
  - Changed Jobs, moved or lost jobs
- Addressed Standardization of format for electronic information transfer and claims
  - For Healthcare Organizations, Insurance plans, Doctors and Patients

What is HITECH Act

- Health Information Technology for Economic & Clinical Health
  - Expands on the HIPAA Privacy Rule
  - Expands on the Security Rule

  ……in protecting Patient Health Information (PHI)
- Increases Patient's Rights
- Protects unauthorized and Commercial use of PHI
- Mandates Breach Notification to OCR
- Also requires Business Associates and Covered Entities to implement effective Information Security Programs

What is ARRA?

American Recovery & Reinvestment Act (Feb 17, 2009)

Subset of ARRA is:

-HITECH Act

What is “Covered Entities”

- Examples of “Covered Entities” are—
  - Dentists & Dental Practices and Referral Specialty Clinics
  - Dental Health Plans/Insurance
  - Pharmacies
  - Healthcare billing and clearing houses
  - Dental Laboratories and Labtechs
  - Other Medical Labs and Pathology Labs & Services
  - Referral Physician’s Offices
  - Information Technology Providers and Remote Back-up Companies, EHR Companies
  - Legal Services Companies
  - Organization where clinic is located– Prisons, JDC, Hospital, Schools

What is a “Business Associate” (BA)

A person or entity performing certain activities or tasks involving use of or disclosure of PHI on behalf of or that provides services to a covered entity.

These covered entities/Business Associates must have a BA contract protecting the PHI as required by HIPAA

These BAs must comply with the HIPAA Privacy and security provision of HITECH Act

What is PHI

- **Protected Health Information**
  - "Any Patient Information that can be linked to a specific patient or narrowed down to a specific patient"……needs specific identifiers or variables
- Examples of Identifiers are—
  - Name, address, DOB, SSN, Telephone #, Health Record#, Photo, Biometrics (Fingerprints), Credit Card Information

  …….with one or more of these we can track down a patient

Types of PHI

- Electronic, spoken, written, heard
  - Billing/Insurance coverage info
  - Chief Complaint of admission/visit
  - Diagnosis of condition
  - Allergies/Alert
  - Observations, Medical/Dental History
  - Medication taken
  - Treatment provided/scheduled
  - Test Results/findings
  - Follow up information

Texas House Bill 300

HB 300 June 17, 2011 "Became Effective September 2012"

- It amends the Texas Health & Safety Code
- Also called Texas Medical Records Privacy Act
- Makes Compliance with PHI a must
- Amends portions of "Texas Identity Theft Enforcement and Protection Act"
- Administered by Texas Health & Human Services Commission (HHSC)

HB 300

- Includes provisions on—
  - Training required for employees of covered entities
  - Consumer/Patient access to PHI
  - Notice if PHI is subject to electronic disclosure
  - Report by the AG regarding consumer complaints
  - Prohibits sale of PHI by covered entities (with certain exceptions)
  - Requires AG to adopt a Standard Authorization Form in complying with disclosure requirement by Jan. 01, 2013

HB 300

- Sets cap and Raises limits on civil penalties with respect to violation of state medical record privacy laws based on certain standards of culpability
- Establishes the powers and duties of the Health & Human Services Commission relating to audits of covered entities
- Amends breach notification provisions

What is a Covered Entity in Texas

- Meaning is always different in Texas

•Who– for professional, commercial, financial gain or fees or dues

•Who– is Cooperative, *pro bono* or non-profit

•Who— engages in the work of collecting, assembling, analyzing, synthesizing, evaluating, archiving, storing, sharing or sending PHI

•Who– receives or possesses any identifiable PHI

•Who –receives, gets or store PHI as under the Texas Act

•Who – is an agent, consultant, contractor, employee or a subsidiary of a covered entity and all of these above roles handles the PHI

Simple words of Covered in Texas

- Under HIPAA definition those classified as—
  - Business Associates & Health Care Payers (insurance), Governmental unit s (State Health Payer or Coverage Programs…eg. CHIP)
  - Healthcare Researchers (Involved in patient care and clinical research)
  - Educational Institutions that may be involved with PHI of students
  - IT units that manage Patient Information or Health Information
  - Healthcare Facility (Hospitals and Healthcare Teaching Institutions)
  - Individual Clinics (Corporations or Sole Proprietership)
  - Website professionals that maintain clinical or patient care facility websites
  - Companies that manage networks, email systems, data storage, internet access

Exemptions to Covered Entities in Texas Act

- May include exemption or partial exemption
  - Employers (who handle employee PHI)
  - Workman's Compensation Program
  - Employee Benefits, Benefit Plans
  - Educational and Treatment Records that fall under the domain of FERPA (Family Educational Rights and Privacy Act)

Breach Notification in Texas

- Any breach in security of sensitive information by—
  - Any of the entities mentioned in the covered entities categories that conduct business in Texas
  - Who own or license electronic health information including critical personal information

  ……..Must Disclose and Notify the Breach to all affected whether a Texas Resident or a Resident of another state
  - That the sensitive information was breached or believes reasonably that there was a breach by an unauthorized person or entity
  - Disclosure to be made ASAP, except when by law requested as delay or if they need to determine the scope of the breach and take remedial action to protect the information for the future
  - For out of state victims, the Texas Act must first be satisfied in addition to the other state's laws and Federal Laws with respect to notifications

Penalties for Breach - Texas

- Maximum $100 Civil Penalty for each Individual's Sensitive Information Breach for Each Consecutive Day of Action Not Taken
- Maximum Total of $250,000 for all individuals for whom notification is due after one breach
- State Attorney General may bring action to recover the monies deemed civil penalties

Training required by HB 300

- All covered entities including all relevant employees must be trained in both Texas State HB 300 and Federal HIPAA Rules of PHI
  - Topic must include the what pertains to the employee's scope of work (differs between different categories of employees) with respect to the entities course of business

Training required by HB 300

- Training to be completed within 60 days of starting employment/duties
- Repeat Initially and Every Two Years
- Signed Attendance Log to be Maintained (electronic or physical log)

Patient Access to EHR

- If a patient requests in writing, information contained in the EHR, you have 15 days to comply
- Provide information in electronic format until and unless patient requires in other formats
- Provider not required to provide access to person's PHI that is excepted from access or to that information that may be denied under 45 CFR, Section 164.524 of HIPAA Privacy Rule.
- TX requirement time is shorter than Federal 30 days

What you can do with PHI- Texas

- Cannot share for remuneration
- Only can disclose for –
  - Treatment
  - Payment for services
  - Healthcare Operations/Functions
  - For legal insurance or HMO function as described by the state or federal law
- Only reasonable costs for legitimate transmittal of PHI to covered entities

Electronic Disclosures

- If legitimate sharing of information has to be done, individual must be notified—
  - By posting a written notice at the place of business
  - By posting a notice on the business website
  - By posting in any other place where individual is likely to see the notice
- If there is a need to disclose PHI to any other entity that is not a covered entity, you must obtain Patient Consent, otherwise you cannot disclose PHI
- AG is required to adopt a standard authorization form for this purpose

Audits of Covered Entities

- A covered entity may be audited by—
  - Texas HHSC, AG, Texas Health Services Authority and Texas Dept. of Insurance can request the Federal HIPAA enforcers (to see if there is compliance by the covered entity)
  - There will be periodic monitoring by State Officials of the HHS Audits of Covered Entities
  - May ask them to submit a HIPAA Risk Analysis
  - May ask the State's Licensing Agency to audit for compliance of privacy standards

Need to know RULE

- Only those directly involved with individual patient need to know the patient's PHI
  - Has a bearing on access to all records by all employees or entities
  - Care providers can share Treatment Information for appropriate care of patients (amount of information to be shared left to care provider's professional judgment)
  - Use you judgment and don't share unnecessary information with consultants and other covered entities

Need to know RULE

- All people involved in care do not need to know everything, but should only know and use what is needed (judgment)
- Access only those records of patients that are assigned to you or you are treating in the group practice
- If the patient is not yours, then do not try to access all the information that is in that patient's record that is not meaningful to your provision of care to that patient

Do's & Don'ts

- Avoid unnecessary discussions and gossip anywhere
- Return patient info back to records/storage or destroy temporary info
- Close door/keep voice low/do not announce
- Flip over the patient chart so that no one can see the identity
- Same thing with computer screen
- Wear name tags or IDs and look out for suspicious people/strangers
- Don't take information out of clinic
- Do not use unencrypted mobile devices to use PHI
- Do not email information unless encrypted
- Do not leave PHI items in printer
- Use secure access to computer, email, internet
- Use and update Security Software
- Do not use internet access in open public access places and view PHI
- Lock and Key approach
- Internet & Digital Security
- Do not share passwords
- Whole bunch of stuff needs to be done.

Questions

Exercises in Information Handling

- Financial
- Health
- Other Info
- Lock and Key Measures for Physically Stored Info
- Digital Security
  - Computers
  - Handheld devices
  - Phones

Patient Financial Info

- Financial Info:--
  - Checks
  - Cash
  - Credit Cards
  - Insurance Reimbursements
  - How do you maintain these methods of payment or receipts?
    - Digitally?
    - Physically?
    - Who has access to these?
    - What is the SECURITY and AUDIT Measures do conduct?

Patient Health Info

- Health Info:--
  - Consent is the first thing
  - Is this a referral?
  - How did you get the info (Protected/Unprotected?)
  - Who sent the info to you?
    - Business Associate or other Covered Entity
  - How do you maintain these data during and after treatment?
    - Digitally?
    - Physically?
    - Who has access to these?
    - What is the SECURITY and AUDIT Measures do conduct?
  - How do you send this or other info back to referrer?

Measure for physical info

- Lock and Key Measures for Physically Stored Info (Health and Financial)
  - Where is it stored?
  - Who has access?
  - Who maintains the Key?
  - How do you audit and how often?
  - Were there any breaches?
  - What is the action taken or to take?

Do a walk-through

- Look for Physical Access and Security Breaches
- Can others access the physical info
- Can others see the info on the screens
- Can others see the info on the charts
- Do you call out names loudly
- Do you give out numbers
- Call them to the window and speak softly
- Two people with the same name – Photo needed

Privacy Filters

Do you have these?

Feed the lawn…..feed it.

Measures for digital info

- Digital Security in the Clinic – Internet or Cloud issues
  - Do you have internet access in some computers or all?
  - Is this a unique server located within the clinic?
  - Is the data on a common server located here or elsewhere?
  - Is the data backed up remotely?
- Digital Security in the Clinic (Antivirus, Malicious Software Blocking, Firewall, Protected Email/Internet Access Software?)
  - Computers
  - Handheld devices
  - Phones

Some Software to USE

- Do all your updates (Windows or IOS)
- Windows Defender for monitoring
- Use Antivirus Software that comes with—
  - internet security
  - constant monitoring
  - Checks all removable hardware that you insert (MacAfee, Norton, AVG, AVIRA, Kaspersky……)
  - Cleans all the unwanted junk (C-Cleaner)
  - Settings for browsing should be moderate to avoid all the junk and malicious sites
  - Nothing comes free (except worms, viruses, malicious software that transmits info to hacker)

Software

- Get a Geek once a year or as needed
- Patches and Updates on your system
- Set up File Encryption Software
- Do not use free email such as Google, Yahoo, etc…..although others have shared info (NSA?)
- Teach all dentists that refer to you about file encryption
- Learn file encryption

Some Software Exercises

- File Encryption – Axcrypt
  - http://download.cnet.com/AxCrypt/3028-2092_4-10564424.html?c=SEM-SEO&s=fivemill&pid=dlcom_sem&aid=axcrypt-e&dlc=n&part=fivemill
  - How do we use this…physically make them download and encrypt—
    - Image File
    - CD
    - Drive….
    - Email security and sending a password
    - Phones/Tablets

Secure Email

- Barracuda
- Microsoft Business Class Email
- Rpost
- MailRoute
- Check out security on Cellphones and iPads (go to Apps)
- Make sure all devices are covered within your network
- Make Sure your wifi is protected
  - Separate for clinical use
  - Separate for non-clinical use/patients….

Question and Answers

- Ask me a question and wait for the answer…….