SETMA HIPAA Training

OCTOBER 2ND, 2012

SETMA & The Mayo Clinic

- Some of this won’t be fun. Some might be a little inconvenient.

- When discussions get fragmented or ugly. They bring things back into focus with one simple question....

- **What is best for the patient?**

HIPAA

- It is not just an **IT** thing!

What is HIPAA?

- The Health Information Portability and Accountability Act – 1996
- Two Sections
  - Privacy
  - Security

Privacy

- Privacy primarily defined:
  - Who was covered by HIPAA
  - Defined PHI (protected health information)
    - Name, DOB, SS#
    - Any information that could be linked to an individual
  - How CE could use Patient Data
    - Treatment
    - Payment
    - Operations
  - Defined Patients Rights
    - Notice of Privacy Practices
    - HIPAA Authorization
    - Copy of Chart
    - Accounting of Disclosures

Security

- The Security Rule:
  - ○ Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.
  - ○ Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
    - Requires Policies and Procedures
    - Requires Annual Risk Analysis
    - Requires Implementation of certain technologies

Why haven’t we done this before?

- Originally HIPAA was complaint driven.
  - We did some of it…
  - No real motive to follow expensive, difficult rules.
  - If a patient did not complain…nothing happened.
  - SETMA went 10 years with 1 complaint

What has changed?

- Proactive Audits
  - 20 random audits prior to April 2012
  - 150 random audits between April and End of 2012
  - More to come in 2013
- Holding individuals personally accountable
  - People can go to jail for wrongful disclosures
- Mandatory Self Reporting

What is a HIPAA Audit?

- Show that you have all the policies and procedures required by HIPAA in place.

- Show you have been using them.
  - Training policy, training materials, training rosters.
  - Security incident policy, security incident reports.

- 2-week notice. Once you get notified it is too late to do anything.

Common HIPAA Security Issues

- Lack of Incident Response and Reporting
- Lack of Security Awareness and Training
- Poor Technical Access Control
- Poor Physical Workstation Security

What is today for?

- To Increase our Security Posture
  - Security Posture is your overall security plan to protect from internal and external threats.
  - Employee Training is a big part of a security plan.

Horror Stories

- February, 2011 – $4.3 million fine Cignet Health of Maryland due to HIPAA violations.

- July, 2011 - $865,000 fine UCLA Medical due to employees snooping in charts.

Horror Stories – Cont’d

- June, 2012 - $1.7 million fine Alaska Dept of Health due to loss of hard drive and failure to have proper policies, procedures and training in place.

- September 2012 - $1.5 million fine Boston ENT Clinic due to loss of a laptop and failure to have proper policies, procedures and training in place.

Personal Accountability

- Large fines could impact SETMA’s ability to give raises, bonuses or even continue to function.

- You could be held personally accountable if your failure to follow our policies results in a breach.

Examples of Personal Accountability

- April, 2011 – Alabama. Hospital employee stole 4500 patient accounts intending to commit identity theft. Faces 10 years in prison and $250,000 fine per count.

- August, 2012 – New York. Medical Supply company stole information from nursing homes and submitted $10.7 million in fraudulent claims to Medicare. Owner faces 10 years in prison and $250,000 fine per count.

Mandatory Self Reporting

- By Law we have to:
  - ○ Report any breaches to HHS and notify the affected patients.
  - ○ Any breaches involving more than 500 patients we have to call the local news media.
    - This is not how any of us want to become famous in SE Texas.

What is a Breach?

- Misdirected fax, email or hard copy communication
- Lost laptop
- Improperly decommissioned workstation or server
- Improperly disposed patient documents

Primary Concepts

- Minimum Necessary
  - When providing information to a specialist, insurance company, etc. Only include pertinent information.
- Review the Patient’s HIPAA Authorization form
  - This form is for the patient to authorize who we can and cannot talk to. If we don’t check this EACH time we interact with the patient we might as well not have it.
- Life Cycle of Data
  - Data comes in, is used, stored and disposed.
- Don’t email PHI outside of SETMA without encrypting it
  - SETMAPHI

Life Cycle of Data

- Data Comes In
  - Face to Face, Phone, Fax, Mail, Email, CD’s
- Data is Used
  - Use minimum necessary to file claims, approve and coordinate referrals.
- Data is Stored
  - Secure your data that is stored in databases, paper charts, stand alone systems, CD’s, disks, hard drives, etc.
- Data is Disposed
  - Destroy! Shredding paper, formatting and smashing hard drives.

What is SETMA Doing?

- We are training our employees!
- We completed a Risk Analysis and have a plan to fix all issues.
- We are implementing required policies and procedures.
- Encrypting our data
- Auditing our systems

What is SETMA Doing? - Contd

- Introducing Two Factor Authentication
  - Something You Have, Something You Know
  - Smart Card – Small Computer
  - PIN – 5 to 7 digit code
  - Demonstration!
- Important Smart Card Facts
  - You have to have it to logon
  - The card will function as your badge.
  - You will be required to wear it.
  - It will operate the doors.
  - $50.00 replacement cost.
  - Posession – you have to have it to do your job.
    - Forget it at home you will have to go home to get it. This will be done off the clock and you will not be allowed to make up the time.

Passwords & PINs

- Don’t write them down
- Don’t share them
- Passwords should be complex
  - puppies is not a good password
  - !Puppi3s is pretty good
- PINs should not be a birthday or address.
  - They should be random - 458631
  - 111111 or 123456 is not a good PIN

Workstation Security

- Lock your workstation when you leave
- Point your screen where people cant see it
- Use a privacy screen if needed
- Log Off at the end of the day

Policies & Procedures

- We are still in the process of writing and implementing our policies.
- They can be viewed on SETMANET under the IT section.
- Information Security Agreement

Information Security Agreement

I understand that Southeast Texas Medical Associates, LLP (the "Company") in which or for whom I work

- has a legal and ethical responsibility to safeguard the privacy of all patients

- to protect the confidentiality of their patients' health information.

In the course of my employment / assignment at the Company, I understand that I may come into contact with this type of Confidential Information.

- I will access and use this information only when it is necessary to perform my job related duties
- I understand that the company policies are available on the intranet and that I am responsible for reviewing and understanding them and that I will be held accountable for following them.
- **I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.**

IS Agreement – Cont’d

- I will act in the best interest of the Company and in accordance with its policies, procedures and Code of Conduct at all times during my relationship with the Company.

- I understand that I should have no expectation of privacy when using Company information systems.

IS Agreement – Cont’d

- I will not connect unauthorized equipment to the practice's network.

- I understand that I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company.

IS Agreement – Cont’d

- I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and position screens away from public view.

- I will only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

IS Agreement – Cont'd

- I will:
  - use only my officially assigned user ID, password, etc.
  - use only approved licensed software.
  - use devices with virus protection software.
  - report theft or loss of mobile devices (cell phones, PDAs, laptops, etc.) that store Confidential Information within 24 hrs.

IS Agreement – Cont’d

- I will never:
  - share or disclose user IDs or passwords, nor will I ask others to do so.
  - use tools or techniques to break or exploit security measures.
  - connect to unauthorized networks through the Company’s systems or devices.
  - knowingly include, or cause to be included, any false, inaccurate or misleading entry in any record or report.
  - knowingly or carelessly perform an act that could interfere with the normal operation of the Company’s systems or devices.
  - attempt to monitor or tamper with another user's electronic communications or files.

IS Agreement – Cont’d

- I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.

- I will not in any way copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized.

IS Agreement – Cont'd

- I will not make unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.

- I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards.

IS Agreement – Cont'd

- I will only access electronic systems to review patient records for which my job responsibilities have a legitimate need to access for treatment, payment or healthcare operations.

- I will notify my manager or appropriate Information Technology person if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

IS Agreement – Cont'd

- Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.

- I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.

IS Agreement – Cont'd

- I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies.

Reporting Violations

- Any person, in any capacity (employee, contractor, external third-party, vendor, business associate, or the public at-large), may report – and <u>has a duty to report</u> – any known or suspected security incident, without fear of reprisal or retribution, and to report it immediately. Reporting of a security incident may be done anonymously if desired. Security issues may be reported to:

Reporting Violations – Cont’d

- the user’s manager or department head,
- the Facility Security Officer (FSO),
- the Corporate Security Officer (CSO),
- the SETMA Corporate Service Desk,
- any member of Executive Management.

Examples of Violations to Report

- Repeated violations of any security policies and standards currently in force by any user (e.g., repeated incidents of password sharing);
- Any security incident which involves the loss of data or inappropriate (accidental, inadvertent, or deliberate) disclosure or dissemination of EPHI.
- Attempted or successful use, disclosure, modification or destruction of data by unauthorized individuals
- Anyone disabling/bypassing information security controls (e.g., firewall bypassed, logging disabled);

HIPAA People

- Privacy Officer – Cindy Bright
- Security Officer – Richmond Holly