HIPAA Security

What Every HIPAA Professional Should Know

Presented by:
Sharon A. Budman, MS Ed, CIPP
Ishwar Ramsingh, MBA, CISSP, CISA, CISM

Thursday, March 29, 2007

Purpose

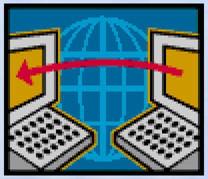
- Provide guidance to IT administrators who manage systems that store and/or transmit electronic protected health information (EPHI) and make EPHI accessible to multiple people

- Useful for department heads/business unit heads who are ultimately responsible for EPHI systems

General Knowledge /Definitions

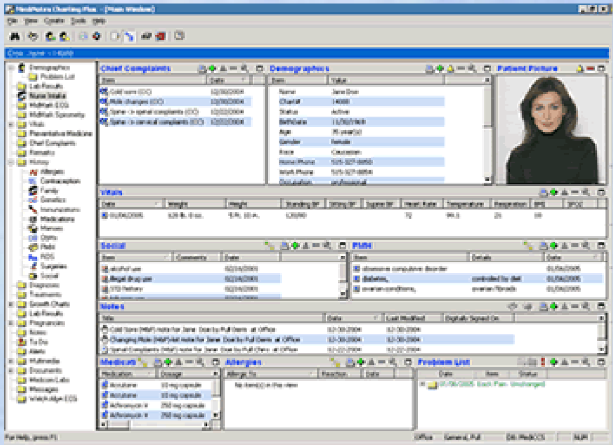
- What is PHI?
- Any information that identifies an individual and relates to one of the following:
  - The individual's past, present or future physical or mental health
  - Provision of health care to an individual
  - Past, present or future payment for health care

- What is EPHI?
- Protected health information which is created, stored, transmitted or received electronically.

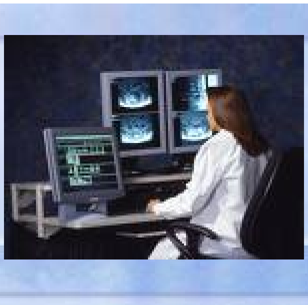


Examples of Data Elements that make Health Information PHI

- Names
- Address
- Phone number
- Medical Record Number
- Health Plan Beneficiary Number
- Social Security Number
- Driver’s license number
- Passport Number
- Email address
- Date of birth
- Photographic images



EPHI Systems



- Traditional data processing systems such as servers that store EPHI
- Clinical care systems/medical devices that store or transmit individually identifiable medical data

NOTE: The distinction between computer systems and medical devices with electronic storage capabilities is decreasing

  - Many medical devices now work in conjunction with network-attached workstation/s and/or may store images/data on a network attached device

Security Rule Focus

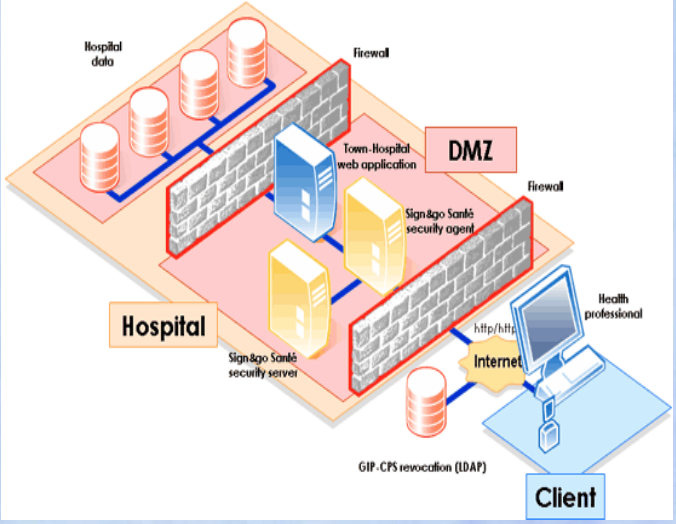
PROTECT

“CONFIDENTIALITY”

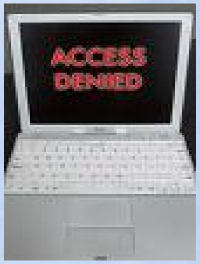
“INTEGRITY”

“AVAILABILITY”

of EPHI


Hospital data
Firewall
Town-Hospital web application
DMZ
Firewall
Sign&go Santé security agent
Health professional
Hospital
http/http
Internet
Sign&go Santé security server
GIP-CPS revocation (LDAP)
Client

Security Rule Focus



Confidentiality

EPHI is not made available or disclosed to unauthorized persons or processes.

Integrity

EPHI has not been altered or destroyed in an unauthorized manner

- Integrity ensures that we can rely on data in making decisions

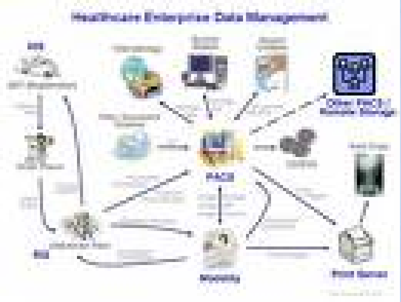
Availability

Systems responsible for delivering, storing and processing EPHI are accessible when needed by authorized persons

Administrative Safeguards

Risk Management

- Comprehensive inventory of all EPHI systems
- Identify risks to these systems


Healthcare Enterprise Data Management
HIS
PACS
Other PACS / Remote Storage
RIS
Modality
Print Server

- Select and implement reasonable, appropriate and cost-effective security measures that address the vulnerabilities
- Create a standard format to gather system information e.g. Standard System Identification worksheet template

System Information

- System Name
- System Purpose
- Data Description
- Popular Name
- Physical Location
- System Owner
- Number of Active Users
- User Community Description
- Administrative Contact
- Technical Contact
- Security Contact
- Hardware Components
  - Device/Host name
  - Device Type
  - Manufacturer
- Software
  - Operating Systems
  - Applications
  - Databases
- IP Address/es
- Connected Internal Systems
- Connected External Systems
- Vendor Contacts
- System Diagram/s

Examples of Risk

- Is the system/device connected to the network?
  - Potentially accessible to any employee (and others, authorized and otherwise)

- Does it have a public IP address?
  - Higher risk compared to private IP address
  - Private IP can still be attacked by insider or compromised, internal machine
- Does the system run commercially available operating systems, databases and applications?
  - Every OS, database, application vendor with varying degrees of regularity releases “patches” that fix issues including security holes
  - If systems are not kept up-to-date with all relevant patches, the risk of compromise is elevated

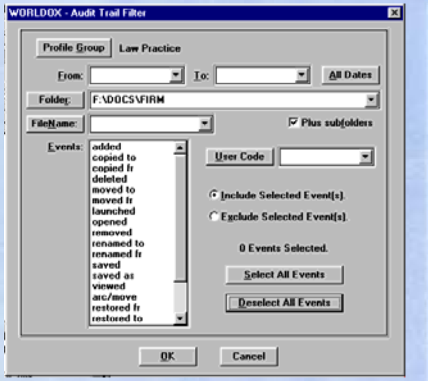
- Is there a risk of disaster (hurricane, fire etc) that destroys your systems?
  - Do you have a Disaster Recovery plan?
  - Do you backup your systems, store tapes at a secure offsite facility, or replicate data offsite?
  - Do you test your Disaster Recovery/restore procedures periodically?

Information System Activity Review

“Implement procedures to regularly review records of information system activity, such as audit logs, access reports etc”

- Do you have audit capabilities in your application and have you enabled auditing, correct?
- Review Access reports
- Don’t just have them, someone needs to review them periodically
- Review Security Incident Reports

Audit Log Contents



Profile Group: Law Practice

Folder: F:\DOCS\FIRM

☑ Plus subfolders

Events:
added
copied to
copied fr
deleted
moved to
moved fr
launched
opened
removed
renamed to
renamed fr
saved
saved as
viewed
arc/move
restored fr
restored to

● Include Selected Event(s).

○ Exclude Selected Event(s).

0 Events Selected.

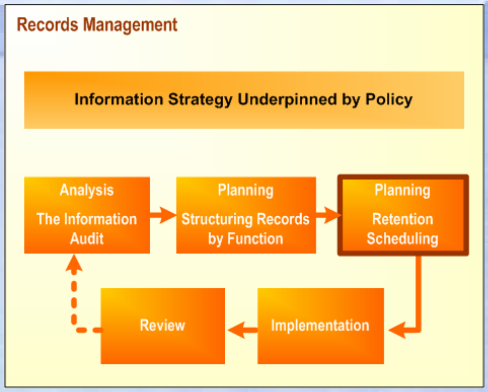
- Date and Time of activity
- Origin of activity
- Identification of user performing activity
- Description of attempted or completed activity

- *Level and type of auditing mechanism should be determined by risk analysis*
- *Logs without proper identification (who performed the activity) and authorization (individual is who he/she claims to be) are useless*

Examples of Audit events

- Access of sensitive data such as patients who are VIPs, HIV results
- Use of a privileged account such as Administrator, root, super-user
- Deletion of files, records
- Changes in level of access
- Creation of new accounts
- Logins, logoffs
- Failed Authentication attempts
- Information system start-up and stop
- Installation/activation of new service

Additional Audit Issues



- How long should audit logs be retained?
  - There is no explicit guidance.
  - At least 6 months – Good rule of thumb
  - Consult with General Counsel/Corporate Compliance
- Document the retention period with Management sign off
- Audit logs may be archived to CDs, DVDs
- Restrict and protect access to these logs
- If there is an incident, especially involving external authorities, logs may become “legal records”
  - NO one should be able to clear logs, without itself writing an event
  - Savvy intruders will attempt to erase traces of their activities
  - Look for gaps in logs i.e. no events for a time period

Assigned Security Responsibility

- Explicit (documented) assignment of responsibility for information security of each EPHI system
  - Can be an individual or group
  - This can be the hands-on person/s
  - Should not be the Clinician/Lab Tech etc unless this person also has IT background/training
- Should ensure each system is patched with all relevant security updates, review access logs, liaise with vendors, other campus IT security personnel etc.

Access Authorization

SEQUEL Field Level Authorization - ASC404

Current Rule

Exclusion Users with *SEQUEL authority are NOT allowed to use the registered libraries, files and fields.

Field Name: CRLIM
Attribute: Pkd 9,0
Description: Credit limit in dollars

- Document procedures for granting access to your EPHI system
- Only grant access minimum necessary access
  - Don’t give “administrator” or “super user” credentials to a user who does not need it
- Don’t just have a document - Follow the procedure
- Conduct formal reviews of who has system access
  - Document and perform regularly at set intervals
- Remove access for terminated work force members and vendors, as well as transfers who no longer are authorized to access such systems.
- Assign unique identifiers to each user
  - Avoid use of generic accounts – simplifies auditing

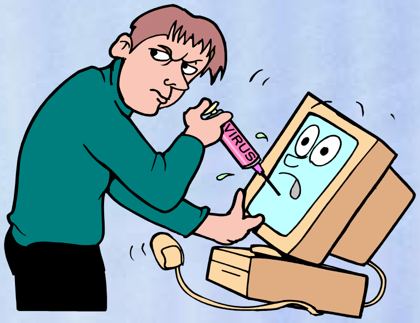
Security Awareness & Training

- Train all users on security features of your systems
  - Use a combination of characters and numbers for passwords or two-factor authentication
  - How to change passwords (enforce periodic change)
  - Display last login date and time
  - How to report suspicious activity

- Make users aware of potential threats, good practices
  - Sign on messages, warning banners, emails, newsletters etc
- Make sure you are staying up-to-date and aware of potential threats to your systems
  - Get on application, OS, Vendor & other security notification lists e.g. SANS, CERT, Microsoft, HP, Symantec, Oracle
- Make your users aware of Social Engineering

Protection from Malicious Software

- Make sure workstations and servers, especially Windows machines have antivirus software



- Update antivirus software daily
- Run regular scans
- Check for security updates for operating systems, databases and applications regularly and apply as necessary
  - Remember to check with and get OK from vendors as appropriate
  - Especially for medical devices governed by FDA rules
  - If you cannot apply patch because vendor has not certified it, then come up with alternative strategy
    - Network Access Control List
    - Internal firewall with appropriate rules

Security Incident Procedures

- What is a security incident?
  - The attempted or successful unauthorized access, modification or destruction of information

OR

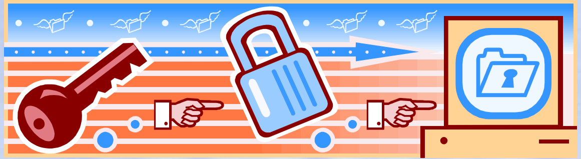
  - Interference with system operations in an information system
    - e.g. making the system unavailable, installing unauthorized files, software, services

Security Incidents

- Examples of incidents
  - Discovery of unauthorized user account
  - Discovery of unauthorized service like FTP
  - Virus/ Trojan
  - Deliberate, malicious act that causes system to be unavailable
  - Discovery of unauthorized access, modification or change
  - Loss of laptop, USB drive with EPHI

Security Incident Procedures

- Depends on your structure and resources
- Classify incidents e.g. Categories I, II, III and IV
  - Category I – little or no potential of adverse effects on the confidentiality, integrity and availability
    - Virus detected and quarantined on single machine
    - Non-criminal inappropriate content on single machine
  - Category IV – Crisis/Emergency Management required
    - Shutdown of patient care or business operations
    - Extreme damage to reputation and/or revenue
- Have a Standard Security Incident Report form



Security Incident Procedures

- Each dept/business unit could have a local security incident response team (LSIRT)
- These are the first responders to security incidents i.e. the system is down, not responding normally or “hacked” with potential for damage (patient care/liability, financial, reputation etc) to the Institution
- In some cases a “team” could be one System Administrator and his/her Manager
  - You probably already have this – it may just not be a formal structure – document it

- LSIRT responds to Categories I and II incidents
- Higher level Incident Response Team (ESIRT) responds to Levels III and IV
  - This team will include Senior Management, General Counsel, Risk Management etc.

Contingency Plans

- Establish policies and procedures for responding to an emergency
  - Example fire, vandalism, system failure and natural disaster
- Develop and document disaster and emergency recovery strategies consistent with business objectives and priorities

Elements of a Contingency Plan

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan
- Testing & Revision Procedure
- Applications & Data Criticality Analysis

Data Backup Plan

- Identify systems to be backed up
- Identify backup schedule and retention periods
  - Satisfy legal, regulatory requirements at minimum
- Identify where backup media are stored and who may access
  - Onsite, offsite, restrict physical access, environmental controls, encryption
- Describe restoration procedures
- Assign responsibility for backup of each system
- Perform test restores periodically

EPHI Disaster Recovery Plan

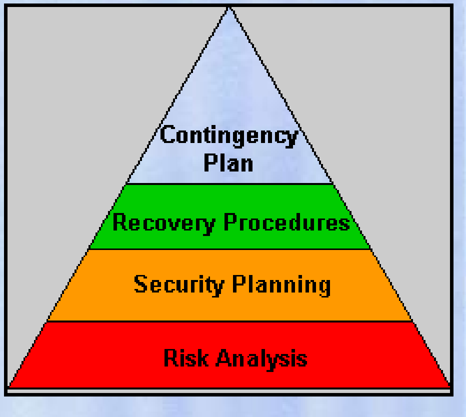
- Your EPHI Disaster Recovery Plan should be a subset of your Dept/Business Unit Business Continuity/Disaster Recovery Plan

- Plan should contain conditions for activation
  - Identification and definition of workforce member responsibilities
  - Resumption procedures
  - Order in which each information systems should be recovered
  - Alert procedure
  - Emergency communications procedure

Other Elements of Contingency Plan

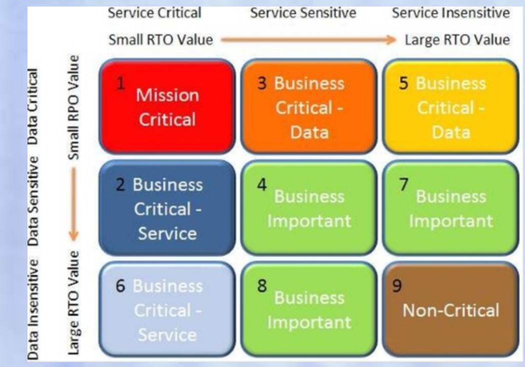
- While operating under any type of emergency conditions, you must still have processes in place to safeguard EPHI

- Should periodically test contingency plans
  - Paper test
  - Limited scope test
  - Simulated full scale test
    - Need Senior Management approval as may involve bringing down primary systems, running off alternate site etc



Application and Data Criticality Analysis

- Complete inventory of EPHI systems under your control
- Identification of relationships between systems, including dependence on non-EPHI systems
- Impact on covered entity services, processes and business objectives if system/s is unavailable
- Identifies which systems are highest priority and order of restoration



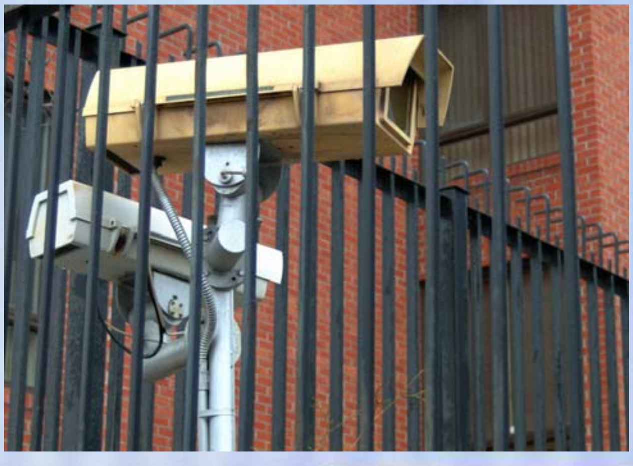
Small RTO Value → Large RTO Value

Small RPO Value → Large RPO Value

	Service Critical	Service Sensitive	Service Insensitive
Data Critical	1 Mission Critical	3 Business Critical - Data	5 Business Critical - Data
Data Sensitive	2 Business Critical - Service	4 Business Important	7 Business Important
Data Insensitive	6 Business Critical - Service	8 Business Important	9 Non-Critical

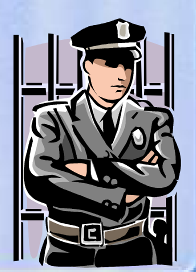
Physical Safeguards

- Facility Access Controls
- Implement measures to limit and/or monitor physical access to EPHI systems and the facilities in which these systems are housed
- Measures include badge readers, key locks, surveillance cameras, alarms, visitor badges



Physical Safeguards cont'd

- Review facility access permissions and update periodically
- Sensitive areas require more controls and frequency of review
- Document who should have access to facilities in cases of emergencies
- You MUST liaise/coordinate with Physical Security
  - Unless you are a progressive entity with unified Physical and IT Security



- Coordinate with your facility administrators

Workstation Use

- All workstations that access EPHI should have a means of uniquely identifying each user
  - Crucial for auditing purposes
  - No sharing of usernames or passwords

- No unlicensed, unapproved software
- Updated antivirus and other anti malware with regular (daily) scanning
  - Educate users on Spyware and deploy anti-spyware solutions
  - Antivirus software does not necessarily protect against spyware
  - Strategically locate workstations so that sensitive data is not displayed to non-authorized individuals
  - Implement password protected screensavers that blank/obscure screens where appropriate
  - Implement time-outs where appropriate
  - Terminate/close sessions after period of inactivity – 15 minutes or less recommended)

Portable Workstations/Media

- Laptops should be secured when unattended
  - In locked offices, cabinets etc
  - By cable
  - ***Laptop loss is a major problem***
    - ***Do not pretend the problem does not exist and ignore it – educate your users***

- Avoid storing EPHI on laptops or other portable media unless necessary
- Obtain permission from system owner before copying EPHI to portable device
- Use encryption to protect any sensitive data on laptops, USB drives

Device/Media Controls

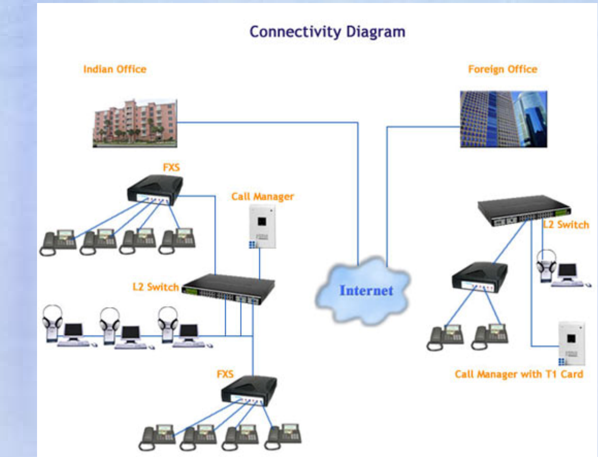
- Have a procedure for safely disposing (i.e. irretrievably erasing) of EPHI
- Do not just throw CDs, optical disks, biomedical devices with electronic storage capabilities etc into the trash
- If you give biomedical devices to Surplus/Environmental Services, then ensure that you have this documented
- If you are giving your old PCs to another department, you should ensure that all sensitive data is removed
- Any device/media being transported offsite or to another facility should be appropriately tracked
- Devices/media "disappearing" with unencrypted, sensitive data is a major issue

Transmission Security

“Implement technical measures to guard against any unauthorized access to EPHI being transmitted over an electronic communications network”

Any communications of EPHI (any sensitive data), to a network outside of covered entity should be encrypted

e.g. Email, Web (http), FTP, Telnet



Transmission Security Cont’d

- Web – Are you using web-enabled applications to transfer EPHI outside the institutions network?
  - You should be using SSL website e.g. https://clinician.webmd.com/jsp/portal/login.jsp
- Do not sent unencrypted sensitive data by FTP or encrypt the data before using FTP
- Do not allow Telnet from outside of your network into your systems
- For vendors and other authorized users who regularly require connections into your systems use VPN tunnel connections, SSL Citrix access or similar encrypted connections

Email Issues

- Avoid including sensitive data in regular email
  - e.g. Do not send email with subject “Appointment reminder for AIDS Research Clinic”
  - Email Reminder “Appointment for Clinic” is OK
- Remember emails can be forwarded to anyone accidentally or otherwise – inside and outside organization

- Follow the Minimum Necessary rule
- Best practice is to encrypt if it contains sensitive data
- **NEVER** send HIV, substance abuse or mental health information in regular, unencrypted email
- Double check long email trails – make sure sensitive, unnecessary data is not being included when forwarded

Email Issues Cont’d

- Make use of Email disclaimer
  - Consult General Counsel for appropriate language
- Do not use Instant Messaging for e.g. MSN Messenger, Yahoo Messenger, AOL Instant Messenger to exchange EPHI or any sensitive data
- Do not use your non-corporate account to send or receive EPHI
  - e.g. Hotmail, Gmail
- Educate your users

Conclusion

- Information Security is everyone's responsibility.
- Your organization will be only as strong as its weakest link
  - You can have strong technical security measures
  - If your users are susceptible to Social Engineering then you are vulnerable
  - 100% security not possible
- Understand the concept of Risk Analysis/Management
- Understand the threats to your systems
  - Understand the importance/criticality of your systems and prioritize
  - Devote more attention/resources to the most critical systems
- Do not neglect the less important systems
  - These systems can be compromised and then used to attack the more important ones

“If you don’t build security into your culture, then you will never be able to hire enough security police to make your enterprise secure”

Mary Ann Davidson
Chief Security Officer
Oracle Corp

Questions/Comments?