The Devil is in the Details: *Implementing a HIPAA Security Compliance Plan*

The Health Colloquium at Harvard

Healthcare Computing Strategies, Inc.

Tom Walsh, CISSP
Practice Manager, Enterprise Security

Security Standards

ADMINISTRATIVE PROCEDURES	
REQUIREMENT:	**IMPLEMENTATION:**
1. Certification	
2. Chain of trust partner agreement	
3. Contingency plan (all listed implementation features must be implemented).	Applications and data criticality analysis. Data backup plan. Disaster recovery plan. Emergency mode operation plan. Testing and revision.
4. Formal mechanism for processing records.	
5. Information access control (all listed implementation features must be implemented).	Access authorization. Access establishment. Access modification.
6. Internal audit	
7. Personnel security (all listed implementation features must be implemented).	Assure supervision of maintenance personnel by authorized, knowledgeable person. Maintenance of record of access authorizations. Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
8. Security configuration mgmt. (all listed implementation features must be implemented).	Documentation. Hardware/software installation & maintenance review and testing for security features. Inventory. Security Testing. Virus checking.
9. Security incident procedures (all listed implementation features must be implemented).	Report procedures. Response procedures.
10. Security management process (all listed implementation features must be implemented).	Risk analysis. Risk management. Sanction policy. Security policy.
11. Termination procedures (all listed implementation features must be implemented).	Combination locks changed. Removal from access lists. Removal of user account(s). Turn in keys, token or cards that allow access.
12. Training (all listed implementation features must be implemented)	Awareness training for all personnel (including mgmt). Periodic security reminders. User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. User education in password management.

*You can have **Security** without **Privacy**.*
*However, you cannot have **Privacy** without **Security**!*

Security Standards

PHYSICAL SAFEGUARDS	
REQUIREMENT:	**IMPLEMENTATION:**
13. Assigned security responsibility	
14. Media controls (all listed implementation features must be implemented).	Access control. Accountability (tracking mechanism). Data backup. Data storage. Disposal.
15. Physical access controls (limited access) (all listed implementation features must be implemented).	Disaster recovery. Emergency mode operation. Equipment control (into & out of site). Facility security plan. Procedures for verifying access authorizations prior to physical access. Maintenance records. Need-to-know procedures for personnel access. Sign-in for visitors and escort, if appropriate. Testing and revision.
16. Policy/guideline on work station use	
17. Secure work station location	
18. Security awareness training	

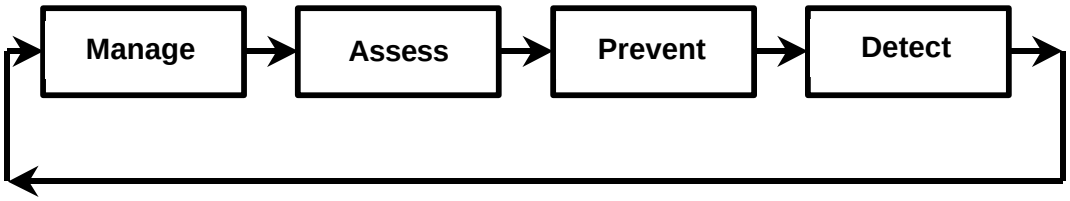
TECHNICAL SECURITY SERVICES	
REQUIREMENT:	**IMPLEMENTATION:**
19. Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
20. Audit controls	
21. Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access.
22. Data Authentication	
23. Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometrics. Password. PIN. Telephone callback. Token. Unique user identification.

TECHNICAL SECURITY MECHANISMS TO GUARD DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK	
REQUIREMENT:	**IMPLEMENTATION:**
24. Communications/network controls If communications or networking is employed, the following implementation features must be implemented: Integrity controls; and Message authentication. In addition, one of the following implementation features must be implemented: Access controls, or Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, & Event reporting.	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

Elements of a Security Program

"Secure your enterprise and compliance will follow." – Steve Hunt, GIGA 12/99

Four Cycle Process of Security:



A security management process encompasses the creation, administration and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches. It involves risk analysis and risk management, including the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic.

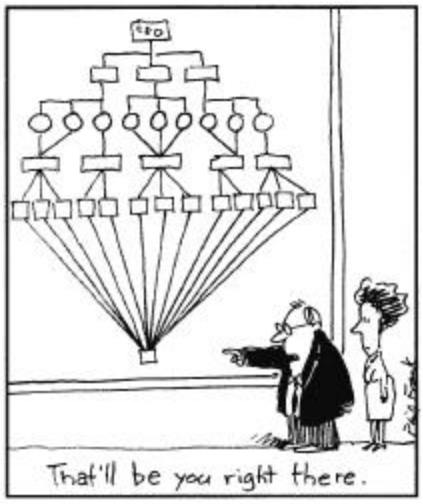
Manage	1. Roles & Responsibilities
(Planning and hiring)	2. Policy & Procedures
Assess	3. Readiness Assessment
(Organizing)	4. Access Controls
Prevent	5. Contingency & Disaster Recovery
(Directing)	6. Certification of Systems
	7. Configuration Management / Change Control
	8. Guideline Workstation Use
	9. Training, Education & Awareness
	10. Business Associate Contracts / COT
Detect	11. Audit Trails, Controls & Alarms
(Controlling)	12. Incident Reporting & Handling

According to the FBI and the Computer Security Institute, the single greatest threat to computer systems is employees.

Almost ¾ of all computer security incidents are caused by an unintentional employee action.

Manage

Roles and Responsibilities



You'll need to assign:

_____

_____

Must have authority as well as responsibility
Can be the same person but...
    Recommend different individuals
Does not have to be an employee

Policies and Procedures

What are the fallacies of policy?
Why do people intentionally break policy?

_____

_____

_____

- *75% of companies do not keep security policies current*
- *Less than 50% of policies are aligned with business goals*
- *Only 9% of employees understand their company's security policies*

Policies

- Review existing policies
- Update as needed
- Create new policies
- Educate everyone
- _____

Policies

- **Subject**
- **Statement of purpose**
- **Policy statement**
- **Definitions**
- **Effective date**
- **Revision date**
- **Authorization**

Assess

Readiness Assessment

- Review selected documentation
- Interview key personnel
- Observe selected operational practices
- Compare existing capabilities against the security and privacy standards
- Review how patient information is processed, stored and transmitted
- Assess vulnerabilities and readiness
- Determine your organization's risk aversion
- Begin HIPAA compliance planning

Mapping the Flow of Patient Information

Few people understand the complexity of the health care environment and who all may have access to their medical information.

Access Control

- Physical
- Logical (UserID / Password)
- Remote (two-layer)

Logical

- UserIDs and Passwords
- Badge, Smartcard, Token
- Biometrics
- Central administration of security controls
- Single Sign-On

Strong Authentication *is based upon combined any two of the following:*

- *Something you know (passwords, PIN)*
- *Something you have (badge, smartcard, proximity cards, tokens)*
- *Something about you (biometrics)*

Remote Access

List organizations or individuals that may have remote access into your information systems that contain patient information.

Medical Equipment

What types of biomedical equipment or other devices store or transmit patient information? Who has access to the equipment?

Prevent

Contingency and Disaster Recovery

- Applications & data criticality analysis
- Data backup plan
- Recovery plan
- Emergency mode operation plan
- Testing and revision

Certification of Systems

To ensure a minimum amount (baseline) of security is in place.

The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external-accrediting agency.

Part of administrative procedures to guard data integrity, confidentiality, and availability.

- Identify system and owner
- Type of information
- Determine the criticality
- Security controls implemented
- Approval

Configuration Management

- Documentation
- Change control
- Security testing (
  - After significant changes
- Anti-virus updates
- Malicious Code
  - Security advisories, bulletins, alerts
- Viruses
- Countermeasures:
  - Anti-virus software (servers & workstations)
  - Patches (specific “fixes” to a problem)
  - Service Packs (upgrades to operating systems)

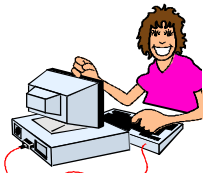
Advisories & Fixes

Bugtraq
www.securityfocus.com

SANS Institute
www.sans.org

Are there procedures for the implementation of software patches and security advisories?

Guideline on Workstation Use



Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings, of a specific computer terminal site or type of site, dependant upon the sensitivity of the information accessed from that site.

Part of Physical safeguards to guard data integrity, confidentiality, and availability on the matrix.

- Information protection (Log off)
- File storage and deletion
- Disposal procedures
- Monitor position

"Donut Strike!"

Training, Education and Awareness (TEA)

- **Training** = _____
- **Education** = _____
- **Awareness** = _____

Business Associate Contracts

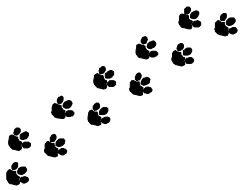
Covered entities are required to enforce their contracts once they are aware of a breach of confidentiality.

- Prohibited from further use or disclosure beyond the purpose stated in the contract
- Required to maintain safeguards
- Report any misuse or unauthorized disclosure
- Subcontractors are held to the same restrictions
- Return or destroy all protected information at the time of termination of the contract
- Agreement can be terminated if there are repeated misuses
- Subject to audit from Health and Human Services.

Detect

Audit

- Trails
- Alarms
- Controls



Audit Trails

An audit trail is a series of records of computer events, about an operating system, an application, or user activities. Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

HIPAA security requirements do not specify the details for generating or maintaining audit trails except that an organization must have them at some level.

Things organizations need to consider when establishing audit trails:

- What to audit and what is the purpose of audit trails (Balanced approach – perhaps audit by exception)
- The granularity of the audit trails (i.e. tracking access to record or to individual data fields within a record)
- The impact on system performance because of audit trails
- An intelligent program or tool for sifting through the data, looking for trends
- Storage and retention of audit trails (Consider the media used for storage)

When you do turn on audit trails, be sure to look at the data!

Incident Report and Handling

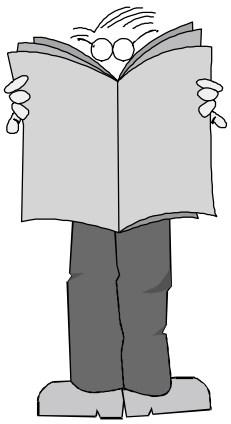
- ***Can associates identify an unauthorized use of patient information?***
- ***Do associates know how to report security incidents?***
- ***Will associates report an incident?***
- ***Do those investigating security incidents know how to preserve evidence?***
- **Goals:**
  - Identify
  - Contain
  - Correct
  - Prevent

- **Provides a way for users to report unusual occurrences or breaches in security or patient confidentiality**

Forum of Incident Response Teams *(FIRST) – Government organization to handle computer security incidents and to promote preventive activities*

www.first.org/

Resources for Additional Information



- Healthcare Organizations - AHIMA, HIMSS, CHIME
  - Web site for security policies:

http://www.sans.org/newlook/resources/policies/policies.htm

  - Healthcare Information Security web sites:

http://aspe.os.dhhs.gov/admnsimp/ (HHS - HIPAA legislation)

http://www.healthexec.net/html/hipaalert.html (HIPAAlert)

http://www.epic.org/privacy/medical/ (Electronic Medical Record Privacy)

http://www.netreach.net/~wmanning/ (Health Law Resource)

http://www.healthcaresecurity.org/ (Forum on Privacy and Security)

Conclusion

- **Everyone is still struggling along – No organization can claim to be "compliant" because the final rules are not published.**
- **Get started now by building a good security program and HIPAA compliance will follow.**
- **Take a practical, reasonable approach.**
- **Documentation is key to proving compliance.**

Final Thoughts

It is my hope that this presentation served your needs. I welcome your feedback. If I can be of help to you in the future, please contact me at:

E-mail: trwalsh@hcs-is.com

Voice: (913) 696-1573

Thanks for attending!

Appendix A - Glossary

ACL	Access Control Lists (Generally a list of users with privileges to a system.)
Audit Trail	Record of events, usually tracked by subject or object. (EX: Users' failed logon attempts.)
Authentication	Verification of the identity of a user or other entity as a prerequisite to allowing access to computer resources.
Authorization	Granting a user the right of access to computing resources, programs, processes, and/or data.
Biometrics	The biological identification of a person, which includes eyes, voice, handprints, voice, fingerprints and hand-written signatures.
BIOS	Basic Input Output System – An essential set of routines in a PC, which is stored on a chip and provides an interface between the operating system and the hardware.
Certification	Formal written assurance that a system meets specified security controls.
CIA of Information	Confidentiality, Integrity and Availability
CISSP	Certified Information System Security Professional
COTS	Commercial Off-The-Self – Commercially produced software programs.
DDOS	Distributed Denial Of Service – An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted.
DSL	Digital Subscriber Line – A technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office.
EDI	Electronic Data Interchange (Computer to computer transactions)
Encryption	The process of transforming information into unintelligible form in such a way that the original information cannot be obtained without using the inverse decryption processes.
HHS or DHHS	U.S. Department of Health and Human Services
Incident	An unusual occurrence or breach in the security of a computer system.
Likert Scale	Likert scale represents a numerical value to an answer to statements rating the strength of the response.
Malicious Code	Computer viruses, Trojan horses, Worm, etc.
Power-On Password	Computer system will not boot without this password entered first.
Risk Assessment	Identification of resources, and the threats to those resources and the vulnerability to those threats.
Sanitization	Elimination of confidential or sensitive information from a computer system or media.
SSO	Single Sign-On – Single authentication to several IT systems
TEA	Training, Education and Awareness
VPN	Virtual Private Network

This page intentionally left blank.