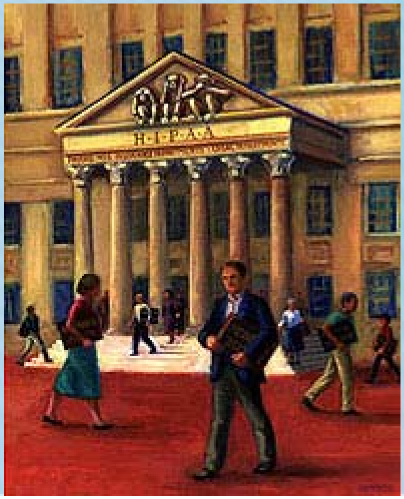
The Eleventh National HIPAA Summit™

The Leading Forum on Healthcare Privacy, Confidentiality, Data Security and HIPAA Compliance



HIPAA Compliance

Keeping it current

Sharon Budman BBA, MS.Ed, CIPP

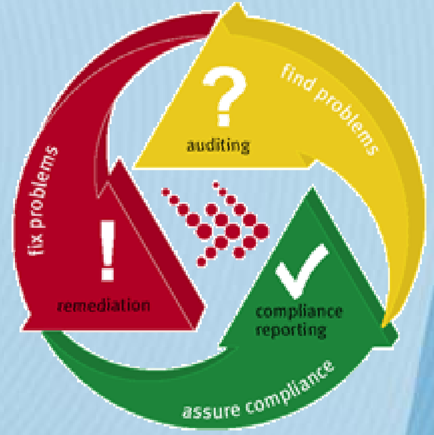
Ishwar Ramsingh MBA, CISSP, CISM

What is Compliance?

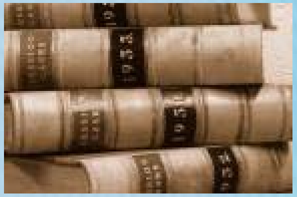
"The ability to reasonably ensure conformity and adherence to organizational policies, strategic plans, procedures, laws, regulations, and contracts."

How is it Achieved? $$

- Policies and Procedures
- Training
- Auditing – Reporting - Certification



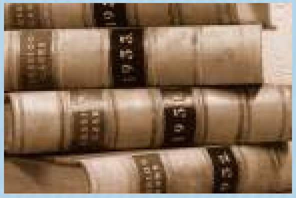
Legal & Regulatory Requirements



- **Privacy Rule §160.308: Compliance Reviews**
  - **"The Secretary may conduct compliance reviews to determine whether covered entities are complying with the applicable requirements."**
- **Privacy Rule § 160.310 Responsibilities of Covered Entities:**
  - **Provide records and compliance reports**
  - **Cooperate with Complaint investigations and compliance reviews**
  - **Permit access to information…pertinent to achieving compliance**

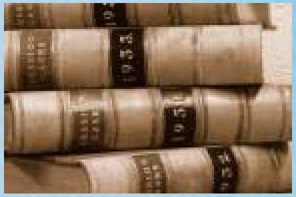
Legal & Regulatory Requirements

- Security Rule, §164.308(a)(1)(ii)(D):
  - *Information system activity review:* "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."



- Security Rule § 164.306(e):
  - *Maintenance:* "Security measures implemented to comply with standards…must be reviewed and modified as needed to continue provisions of reasonable and appropriate protection of electronic protected health information…"

Legal & Regulatory Requirements



- Security Rule, §164.308(a)(2)(8):
  Evaluation

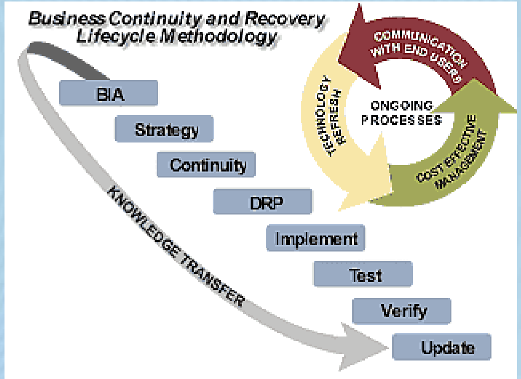
  "Perform a periodic technical and non-technical evaluation, ……, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule."

- Security Rule, §164.312(1)(b):
  Audit Controls

  "Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI."

Compliance
Not just the law - It's good business

- Cost Savings - avoid penalties for non-compliance
- Build Patient Trust - demonstrate commitment to patients' privacy and preserve business integrity
- Reduce business risks
  - Probability of business interruption
  - Destruction of information assets
  - Damage to brand and reputation
- Loss of accreditation/licensure
- Achieve operational efficiencies and lower costs by streamlining/standardizing processes
- Reduce exposure to liabilities associated with improper handling of PHI



Compliance Motivator

- General Non-Compliance
  - Penalties range from $100-$25,000
- Wrongful Disclosure/Knowingly Misuse PHI
  - Penalties range from $50,000-$250,000 and up to 10 years imprisonment
- DHHS has stated, "Federal law should allow any individual whose rights have been violated to bring an action for actual and equitable relief."

Compliance Enforcement

- **HIPAA Privacy Regulation - DHHS Office for Civil Rights (OCR)**
- **HIPAA Security Rule and Transaction & Code Sets - Centers for Medicare and Medicaid Services (CMS) Office of HIPAA Standards**
- **Current enforcement is a collaborative approach, voluntary compliance.**
- **Private litigation remains a separate and important risk**

HIPAA Compliance

HIPAA is NOT done!

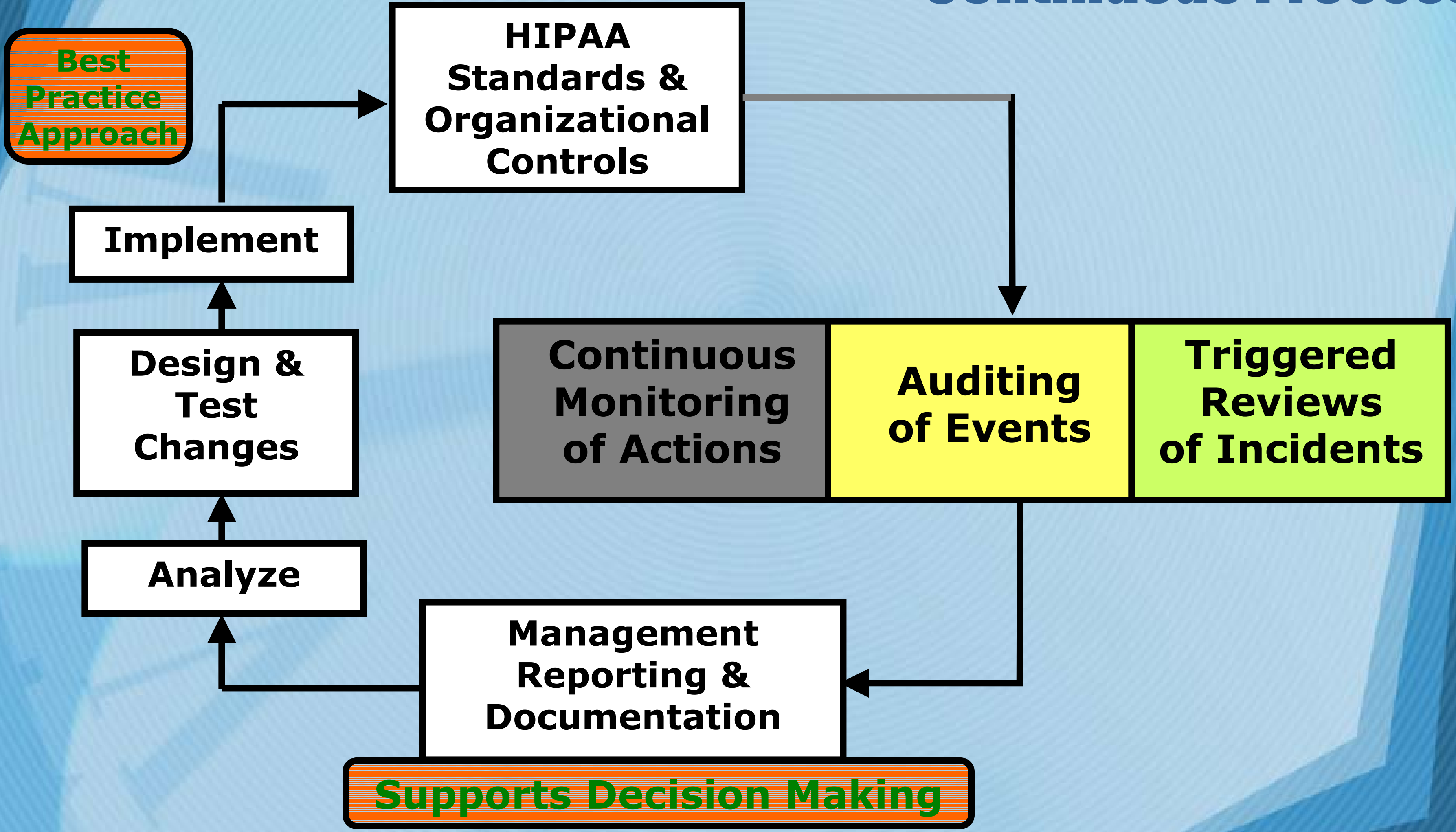
- HIPAA is an evolving process, not a passing event.
- HIPAA compliance with the Privacy and Rules requires on-going efforts from the entire organization.
- The HIPAA process should be an integral part of your organizational healthcare culture.

Compliance is a continuous process

- Businesses change
- New processes continue to evolve
- New policies & procedures are needed as processes evolve
- New technologies are developed
- New information vulnerabilities and threats arise
- New safeguards are developed and implemented as new threats arise
- Compliance today does not mean compliance tomorrow

Compliance Assurance

Continuous Process



Best Practice Approach

HIPAA Standards & Organizational Controls

Continuous Monitoring of Actions

Auditing of Events

Triggered Reviews of Incidents

Management Reporting & Documentation

Analyze

Design & Test Changes

Implement

Supports Decision Making

Assumptions

- Initial risk assessments have been completed?
- HIPAA policies and procedures have been finalized?
- Initial Privacy & Security Awareness Training have been completed?
- Plan for implementation of safeguards has been developed?

HIPAA Compliance - Are we there yet?

It's a continuously evolving process!

- How do we keep it current?
- What are we required to do?

Monitor, Audit & Revise

Monitor - Risk Management

- Risk assessments must be performed regularly
  - Recommended at least once a year
  - Prioritize systems/areas for assessment
  - System changes may result in new vulnerabilities
  - Checklist for new systems before purchase and implementation i.e. build RA into SDLC
  - You are looking for improvement from period to period

- Risk Management – develop and maintain an updated plan to address new vulnerabilities and threats.

Audit Privacy & Security Together

- What are the potential gaps?
  - Lack of Policies and/or Procedures
  - Lack of implementation of Policies/Procedures
  - Lack of education
  - Lack of understanding
  - Lack of awareness
  - Vulnerability to social engineering
  - Lack of consistency in application

- Every department may <u>NOT</u> necessarily have the same procedures.
- The ultimate goal is to find weaknesses and rectify them.

Auditing Basics

- Step 1 – Determine who will be responsible for this function.
- Step 2 - Define the Audit and its objective(s)
- Step 3 – Develop the plan & program
- Step 4 – Perform a preliminary review
- Step 5 - Review the controls
- Step 6 – Perform detailed tests
- Step 7 – Draft a report with recommendations
- Step 8 – Follow-up to ensure appropriate action has been taken based on recommendations.

Auditing Basics

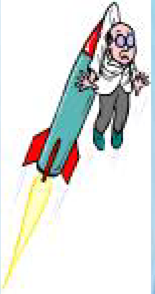
- Who will perform audits?
  - Depends on the size and/or complexity of your organization, consider:
    - Security Officer?
    - IT staff?
    - Managers?
    - Internal Audit?
    - Others, or a combination of those above?
  - By the way, who will audit the auditor?
  - Ideally the audit function should be independent of operational groups

Where to Start???

Consider simple audits:

Structure your program - Example:

Security infrastructure of your security program.

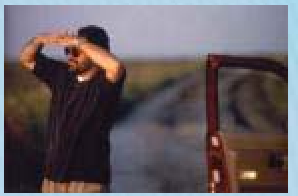


- Do you have in the following in place:
  - Policies and Procedures
    - "how to" guides for staff
  - Forms
    - i.e., security incident reports, new employee access permission forms, termination checklists, etc.
  - Documentation of:
    - Your original risk analysis and updates
    - Your Security Rule Implementation efforts/ decisions
- Review at predetermined intervals (quarterly, annually)

Details to audit – Security Processes

Does your documentation support:

- Workforce members are aware of and know where to find applicable policies and procedures?



- Workforce members know whom to contact if they have questions about specific policies and procedures?
- Most importantly, are policies and procedures followed in practice?

When performing an audit - Use a checklist and an audit program to guide the process.

Auditing the Processes

- Develop an audit program to meet your organizational compliance needs
- Use updated checklists (maintain them by dating all versions)
- Perform periodic unannounced walk-throughs to observe prioritized areas
- Create surveys to use for interviewing workforce members
- Attempt to audit each area/dept at least once a year, if possible.
- High risk and problem areas may need to be reviewed more frequently
- Ideally you want to see improvement from period to period

Auditing can be more than just compliance – it promotes operational effectiveness by standardizing processes!

Checklist/Survey Question Suggestions

- Can workforce members tell you the correct processes/procedures?
- Can they tell you where they can find a policy and procedure if they need to refer to it?
- Can computer screens be easily viewed by unauthorized individuals?
- Do users log off applications when they leave their workstations?
- Are passwords written down in obvious places/spaces?
- Are files left unattended?
- Are medical records in secured areas?
- Do disposal procedures exist for equipment?
- Are disposal procedures followed?

Checklist/Survey Question Suggestions

- Is there evidence that users share passwords?
- Check employee termination lists: Has access to network and e-mail systems been deactivated upon termination?
- Physical Security: Is PHI being disposed of properly?
- Are print-outs kept out of sight of unauthorized viewers?
- Do workforce members know about the security measures such as selecting secure passwords?

Auditing Security Processes
An example…

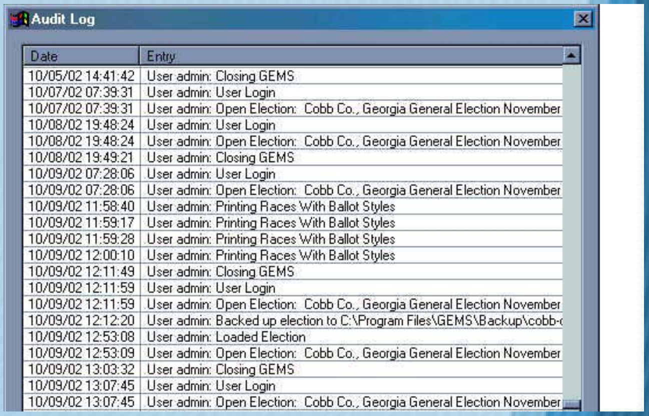
- “Information System Activity Review” - Security Rule, §164.308(D): Required Implementation Specification
  - Considerations:
    - Do your systems produce audit trails?
    - If so, what/how much information is logged?
    - What other tools are available to you in your workplace, i.e. access records and security incident logs?
  - If your organization is a medium-to-large sized covered entity, it is unrealistic to audit every access to a clinical system – PRIORITIZE based on Criticality of the Data.

Looking at Audit Trails??

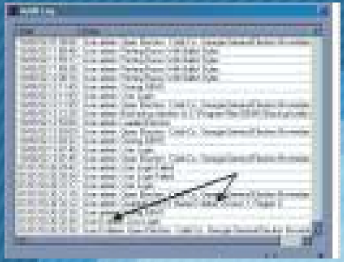
- Audit policy should state how often, and/or under what circumstances, audit/access trails will be reviewed
- Prioritize Reviews
  - Important systems with critical data should be reviewed more frequently
- Review ALL systems periodically
- Who is doing the audit?
  - Do you need to audit the Auditor? Independence is the key.
- The Security Rule does not specify how long you are required to maintain audit trails
  - Clarify with legal and IT – create a policy.
  - Audit trails can grow quickly and significantly
  - Consider archiving to offline storage
  - Logs must be protected from tampering, destruction

What should audit trails contain?
Minimum elements

- Date and time of significant activity
  - Voluminous logging may impact performance of your systems
- Origin of activity
- Identification of user performing activity
- Description of attempted or completed significant activity



Date	Entry
10/05/02 14:41:42	User admin: Closing GEMS
10/07/02 07:39:31	User admin: User Login
10/07/02 07:39:31	User admin: Open Election: Cobb Co., Georgia General Election November
10/08/02 19:48:24	User admin: User Login
10/08/02 19:48:24	User admin: Open Election: Cobb Co., Georgia General Election November
10/08/02 19:49:21	User admin: Closing GEMS
10/09/02 07:28:06	User admin: User Login
10/09/02 07:28:06	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 11:58:40	User admin: Printing Races With Ballot Styles
10/09/02 11:59:17	User admin: Printing Races With Ballot Styles
10/09/02 11:59:28	User admin: Printing Races With Ballot Styles
10/09/02 12:00:10	User admin: Printing Races With Ballot Styles
10/09/02 12:11:49	User admin: Closing GEMS
10/09/02 12:11:59	User admin: User Login
10/09/02 12:11:59	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 12:12:20	User admin: Backed up election to C:\Program Files\GEMS\Backup\cobb-
10/09/02 12:53:08	User admin: Loaded Election
10/09/02 12:53:09	User admin: Open Election: Cobb Co., Georgia General Election November
10/09/02 13:03:32	User admin: Closing GEMS
10/09/02 13:07:45	User admin: User Login
10/09/02 13:07:45	User admin: Open Election: Cobb Co., Georgia General Election November



Practical Suggestions
Audit Trail Reviews

- "VIP" patients (celebrities, physicians, etc.)
- Time of access appears unusual (especially important in web-based record systems)
- Accessing multiple patients by one individual in short time period may indicate patient "browsing"
- Access of one patient by multiple individuals – may indicate "person of interest"
- Last name of patient matches last name of person accessing record
- Pick a patient and check access against treatment record
- Pick a user and verify their need to know in treatment records

Another area to Audit

Security *outcomes*

CSIRT
Computer Security
Incident Response Team

Document and retain:

- Number Security incident reports received and closed
- Number of incidents of unauthorized access found via audit trail
- Mitigation efforts
- Disciplinary actions taken

What to Maintain

- Document your audits and maintain your records
  - First line of defense for support of your compliance efforts in the event of an investigation by the Office for Civil Rights or CMS (6 years)
- Elicit and achieve buy-in from the top executives, clinical and support staff members
  - Compliance
  - Continual process improvement
  - Support of the organizational mission
  - Make it part of the business strategy
  - Improving the bottom line - $$$ - -
    it's all about the business

- Ensure that awareness, education and job-specific training are ongoing and up to date.
  - (Maintain personnel records for documentation of training)

The Audit Report

- Regularly (quarterly/bi-annually) report to Senior Management/Compliance Committee
  - Inform
  - Summarize
  - Be clear, concise, and timely
  - Offer constructive information to
    - Inform
    - Persuade
    - Provide practical means to achieve change.

Remember ….
HIPAA Compliance
Is all about Continual Process Improvement

It makes good business sense!

Keep it current!

Questions?

Thank You !