



Auditing for HIPAA Privacy Compliance

Presented by:

Lesley Berkeyheiser
The Clayton Group
(610) 558-3332

lberkeyheiser@theclaytongroup.org

Mariann Yeager
Emerson Strategic Group
(703)519-0817

myeager@emersonsg.com



Introduction

◆ Purpose

- Share strategies for organizing audit program
- Discussing various approaches given size and complexity of organization
- Build framework that adapts to change

◆ Scope

- Auditing compliance with HIPAA Privacy policies and procedures
- Safeguards – §164.530(c)

What is an Audit?

◆ Auditing

- Objective inspection or review to determine compliance with regulatory requirements and an organization's privacy policies, procedures and processes
- “Snap shot” in time
- Finite activity that evaluates, records & reports findings

◆ Monitoring

- Ongoing routine observation of compliance with daily processes



Why Audit?

- ◆ Reduce and avoid risk
- ◆ Early detection of compliance problems to minimize compliance violations or inappropriate disclosures of PHI
- ◆ Evaluate effectiveness of compliance policies and procedures and internal processes
- ◆ Justify compliance program by demonstrating return on investment



Audit Process

- ◆ Structuring your audit program
 - Type of organization (*type of CE, BA, single entity, hybrid, ACE, etc.*)
 - Size
 - Complexity (*single vs. multi-tiered approach*)
 - Organizational structure (*privacy officer, corporate compliance, internal audit, etc.*)
 - Audit goals & business drivers
 - High risk areas



Audit Process

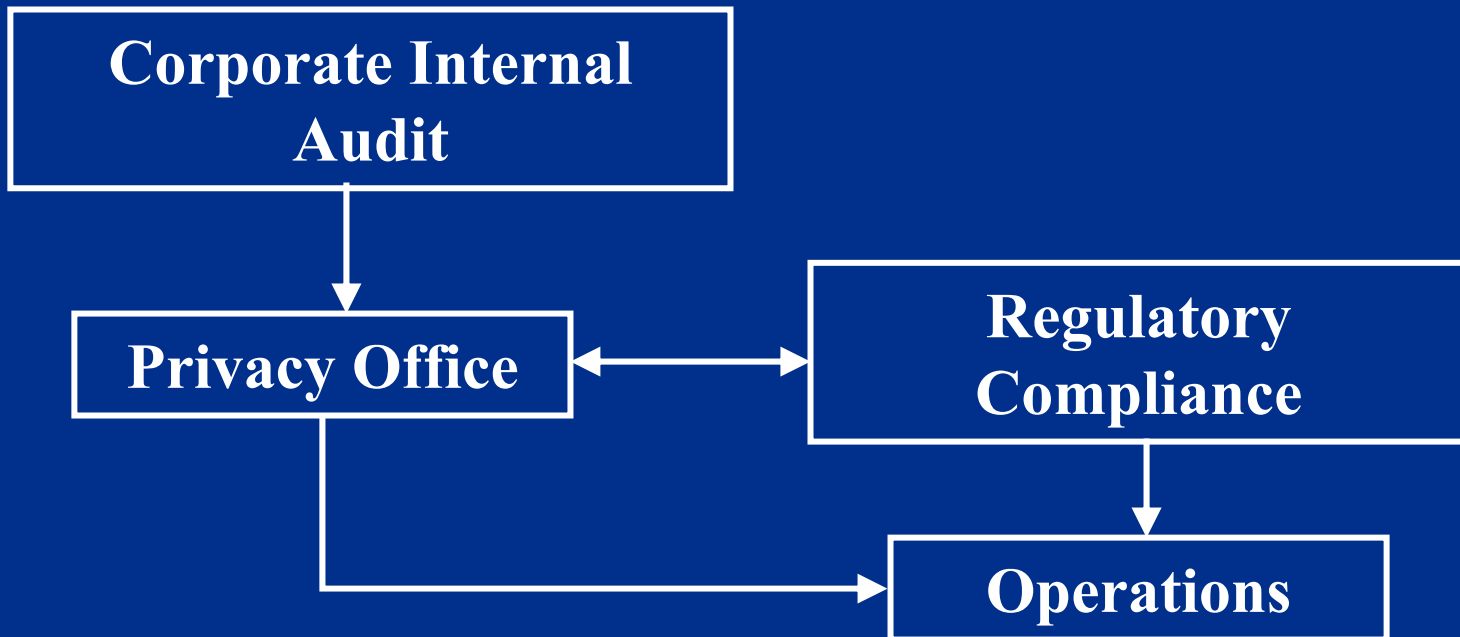
Example: Phased Approach

- ◆ **Phase 1: Review privacy infrastructure**
 - Sufficient and appropriate policies and procedures (P&P)
 - Effective communication and training
 - Process for handling compliance issues
 - Updating P&P and compliance program
 - Ongoing executive buy-in
 - Clear process for maintaining appropriate documentation
- ◆ **Phase 2: Operationalize policies**
 - Documented and implemented departmental P&P
 - Training
 - Additional tools/resources – cheat sheets, etc.
 - Controls and checkpoints
- ◆ **Phase 3: Review workforce compliance**

Audit Process

Example: Multi-tiered Approach

- ◆ Operations / Division – Monitor daily operations
- ◆ Privacy Office – Oversee compliance program
- ◆ Regulatory Compliance Department - Audit operations
- ◆ Corporate Internal Audit - Review Privacy Office





Audit Process

Who should conduct the audit?

Type of Audit	Pros	Cons
External audit services	<ul style="list-style-type: none">• Objective 3rd party.• Can minimize political or peer pressures.	<ul style="list-style-type: none">• May be costly.• May not foster internal accountability for correction and resolution of issues.
Internal audit resources	<ul style="list-style-type: none">• May offer cost savings .• Maintain accountability for ongoing results.• May provide starting point for more formal, external reviews.	<ul style="list-style-type: none">• Potential bias, particularly if same group implements and audits.• Impacts daily operations, unless a dedicated audit team is assigned.• May be reluctant to report issues.



Audit Process

Creating an audit team

- ◆ Determine level of involvement and role of Privacy Official
 - Documentation
 - Validate communication
 - Effectiveness of training
 - Demonstrating ongoing review process and change management
 - Complaint process and resolution
- ◆ Regulatory Compliance group, if applicable
- ◆ Committee approach / multidisciplinary team
 - Regulatory
 - Business / operations
 - Systems
 - Privacy Official

Audit Process

- ◆ Avoiding the pitfalls of internal auditing
 - Clearly defined road map or work plan
 - Clearly communicate expectations and needs for a successful audit
 - Avoid “policing” the organization
 - Constructive audit feedback

Audit Process

- ◆ Don't forget buy-in
 - Support for use of resources and budget to conduct audit
 - Document value of audit (e.g. maximize initial investment in compliance)
 - Identify resources and impact to their daily responsibilities and commitments
 - Set expectations for frequency & timeframes of audits
 - Articulate final deliverables



Audit Process

- ◆ What will you audit?
 - Entire organization
 - Specific departments/functions
 - Specific work processes
 - Individual performance
 - High-level review (verbal interviews)
 - Detailed review (proof of compliance)
 - Targeted risk areas – e.g. based upon exposure to patients or PHI



Audit Process

- ◆ How frequently will you audit?
 - Varies according to scope, resources and budget
 - Examples:
 - Comprehensive audits – every year or two
 - Focused audits – quarterly or semiannually

- ◆ Various methodologies
 - Blind or informed audit
 - Self-audit tool
 - Physical walkthrough
 - Interviews
 - Checklist or scorecard
 - Output samples



Methodology for Auditing

- ◆ To build or buy
- ◆ Define your needs
 - Informal spreadsheet
 - Reports
 - Databases – also used for internal monitoring
- ◆ Evaluate ability to customize and the level of adaptation required
- ◆ Base upon your organization's core privacy policies and procedures



Methodology for Auditing

- ◆ Practical Example:
- ◆ Mid-sized hospital (direct treatment provider)
- ◆ Identify key issue to audit – authorizations
 - Review regulatory requirements
 - Review P&P
 - How was policy communicated?
 - Interview staff
 - Review documentation and tracking

Auditing Results

- ◆ Packaging your results
 - Keep it simple
 - Summarize findings
 - Provide detailed and careful documentation for areas of noncompliance
 - Use lay terms
 - Use charts and graphs to illustrate findings
 - Use executive summaries for senior staff
 - Provide detail to managers
 - Use standard templates for reporting results
 - Review recommendations in person where possible



Auditing Results

- ◆ Who should hear the audit results?
 - Varies by organization
 - Management responsible for addressing areas of non-compliance
 - Workforce members impacted by changes identified by audit
 - HIPAA Committee
 - Executives
 - Board of Directors



Auditing Results

- ◆ Handling violations and non-compliance
 - Provide regulatory citations to support findings
 - Identify new P&P and training needed to resolve the issue
 - Define corrective action plan
 - Address with business manager responsible for that area
 - Senior level management to whom you report audit results
 - Establish work plan or action steps needed to address the issue
 - Provide status reports regarding progress
 - Identify need for re-inspection once changes are implemented



Some Areas for Review

◆ Processes

- Access/Amendment/Designated Record Set
- Accounting of Disclosures
- Assignment/Termination of System Access Privileges
- Sanctions/Breaches/Complaints
- Confidential Communications/Restrictions
- Facility Directory
- Notice of Privacy Practices (Distribution)
- Third Party Relationships (Contracts, etc.)
- Training
- Verification



General Policy

- ◆ Use and disclosure of PHI 45 CFR § 164.506

- ◆ Does the Workforce really understand TPO and when it is ok to use and/or disclose PHI?
 - How can you validate?
 - Interview?
 - Review training curriculum and signoff's?
 - New employee orientation? Test?



Authorization to Use / Disclose PHI

- ◆ 45 CFR § 164.508
- ◆ Standards for form and content of authorization forms
- ◆ Conflicts between authorizations and restrictions
 - Who is responsible to respond to individual requests for authorizations?
 - Major area of operational trouble now
 - HOW= Review records of accepted authorizations against standard elements



Verification of Identity

- ◆ ...and authority of a person requesting disclosure of PHI
- ◆ 45 CFR § 164.514(h)
- ◆ Trouble area:
- ◆ HOW= Perform calls and tests using alias
- ◆ Find out if workforce really know when the procedure to verify identity and when it applies.



Notice of Privacy Practices

◆ 45 CFR § 164.520

- How: Listen to a patient register.
- Note if he/she is provided with NPP.
- Pull a representative amount and look for individual acknowledgement signatures as compared with lists of patients
- What is happening if a guardian is present?
- What happens if the individual refuses to sign?



Accounting of Disclosures

- Required by other law
 - For public health activities
 - About victims of abuse, neglect, domestic violence
 - For health oversight activities
 - For judicial/administrative proceedings, subpoenas, court orders
 - For law enforcement purposes
 - About decedents to Coroners/ME/Funeral Dir.
 - For organ, eye or tissue donation purposes
 - For research purposes
 - To avert a serious threat to health/safety
 - For specialized government functions (military, public benefit programs, etc.)
 - For workers' compensation
- ◆ HOW: You can tell if your organization is tracking correctly if the disclosures (listed above) are logged and compiled in an accounting of disclosures?



Minimum Necessary Rule

- ◆ 45 CFR §§ 164.502(b), and 164.514(d)
- ◆ HOW: Validate training curriculum, ask some test questions...review records areas and consider responses over the telephone.



Assignment/Revocation of Access Privileges

- ◆ Implement P&P to ensure that workforce have appropriate access to ePHI, and prevent unauthorized access (45 CFR §§ 164.308(a)(3) and 164.514(d)(2))
- ◆ Implement procedures for terminating access to ePHI at end of employment. (45 CFR § 164.308(a)(3)(ii)(B))
- ◆ How: Is there a controlling form and/or process? Is there a relationship between job function and access levels?
- ◆ Back track some more recent workforce who have left employment. Do managers confirm access rights revocation? How long did it take to revoke access?



Training program

- ◆ Uses, disclosures, and safeguarding PHI
- ◆ 45 CFR §§ 164.308(a)(5) and 164.530(b)
 - How: Use the results of the audit and other information to determine if the current curriculum is comprehensive enough- if people understand it and are held accountable to comply

Sanctions

- ◆ ...for violating privacy and security policies and procedures
- ◆ 45 CFR §§ 164.308 (a)(1)(ii)(C) and 164.530(e)
- ◆ How: Review responses to breaches/incidents, as well as complaints about privacy practices, both at the workforce level and organization wide



Restrictions & Confidential Requests

- ◆ Requests for Restrictions of use/disclosure of PHI (45 CFR §§ 164.522(a), and 164.502(c))
 - How: Track how many patients have requested restriction?
 - Was the process for review efficient? Did everyone know what to do? Were responses prompt and in writing?
- ◆ Confidential Communications (45 CFR §§ 164.522(b) and 164.502(h))
 - How: Using any post cards lately? Alias policy? Tracking multiple addresses? Billing vs. Clinical
 - Examine process to determine if workforce responding appropriately to reasonable requests



Ways to Reinforce Behavior

- ◆ Safety Committee Reviews?
- ◆ HIPAA Tickets?
- ◆ Acknowledgements?
 - What works in your organization?



Auditing for HIPAA Privacy Compliance

Q&A