

HIPAA Compliance Auditing

Margret Amatayakul,

MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

Margret\A Consulting, LLC

What is Internal Compliance Auditing?

- **Ongoing process for compliance assurance**
- **Specifically,**
 - **Assists in identifying weaknesses to enable establishment of internal controls**
 - **Helps demonstrate commitment to responsible corporate conduct**
 - **Provides accurate view of behavior relative to specific compliance requirements**
- **May be aided by external assessment/consultation, but is not an externally regulated audit**
- **HIPAA requires compliance – which is *ongoing* conformance to laws and regulations**

What Comprises an Internal Compliance Auditing Program?

- **Central source for distributing information about compliance**
- **Methodology that encourages members of workforce to report potential problems**
- **Procedures that allow for prompt and thorough investigation of a problem**
- **Initiation of immediate and appropriate corrective action**
- **Minimizes loss through early detection and reporting**
- **Reduces exposure to (external audits), incidents/breaches, and hence penalties**

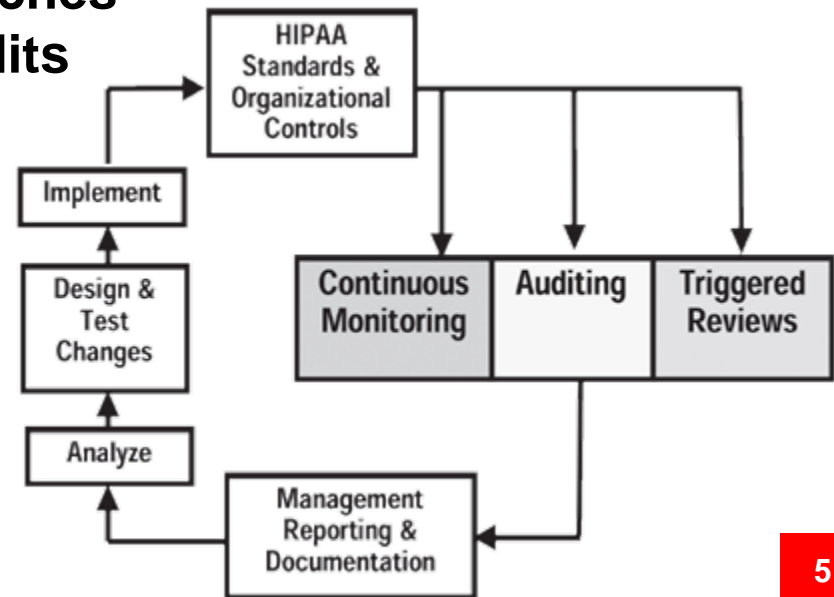
Business Case for Internal Auditing for HIPAA Privacy and Security

- Ever-rising number of privacy complaints to OCR
- Increasing number and amount of settlements for breaches
- Cost of a breach estimated at \$188 per record. Average # of records in a breach = 23,647; or \$4.4M per breach
- Identity theft may be most frequent, costly, and pervasive crime in U.S., with increasing sophistication

43% of identity thefts have a medical component, including potential for treatment and payment errors

Implementing Internal Auditing

- **IPO, ISO, Compliance Officer(s), Risk Manager, legal counsel, develop coordinated program**
- **Determine focus of auditing; use sources such as:**
 - Frequent privacy complaints
 - Known security threats
 - Random spot checks for new vulnerabilities
 - Most common causes of breaches
 - Findings from (OCR/M.U.) audits
- **Create culture of:**
 - Transparency
 - Hold harmless
 - Data stewardship
 - Commitment to risk mitigation



Compliance Assurance Plan Template

Date of Plan:	Prepared by:
Compliance goal:	
Standard(s):	
Owner(s):	
Risk:	
Current Control(s):	
Compliance Process(es):	
Schedule:	
Resources:	
Results:	
Recommendations:	
Follow-up:	

Copyright (c) MargretVA Consulting, LLC; as published in Amatayakul, M. *Guide to HIPAA Auditing*, Third Edition (2014), HCPro.

See handout for sample of completed plan.

Margret Amatayakul

Margret\A Consulting, LLC

Tel. 847-895-3386

margret@margret-a.com

www.margret-a.com