How to prepare your organization for an OCR HIPAA audit

Presented By:
Mac McMillan, FHIMSS, CISM
CEO, CynergisTek, Inc.

Technical Assistance: 978-674-8121 or Amanda.Howell@iatric.com

Audio Options: Telephone 1-562-247-8321 l Access Code 366-675-060
Computer Microphone and Speakers

This teleconference will be muted while we wait for all attendees to join.
Thank you for your patience.

Webinar Guidelines

Technical Assistance

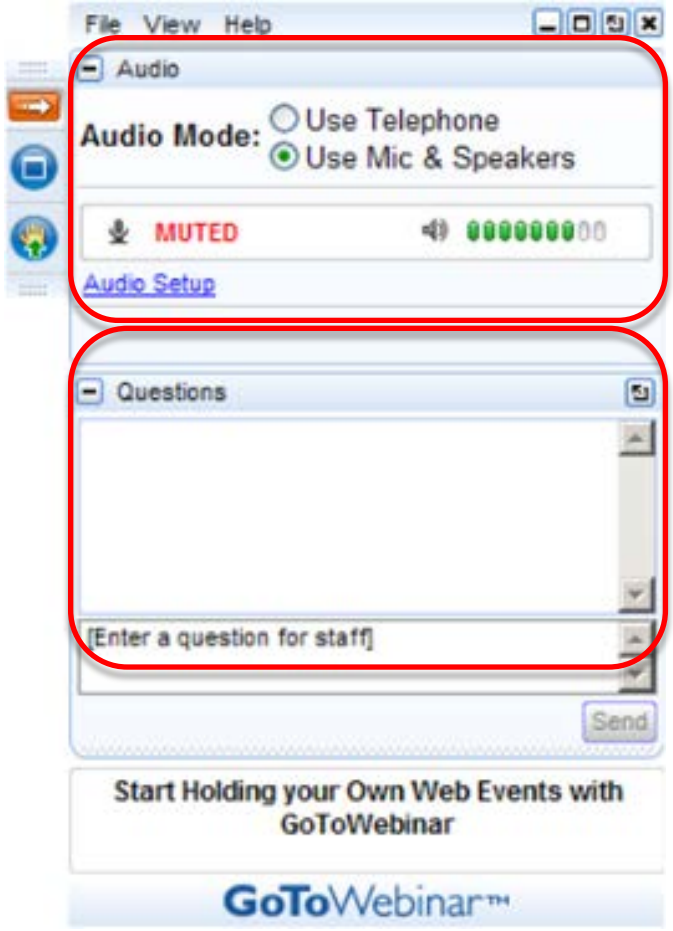
- Amanda.Howell@iatric.com
- 978-674-8121

Participation

- Select preferred Audio Mode
- Submit text questions
- Recorded session

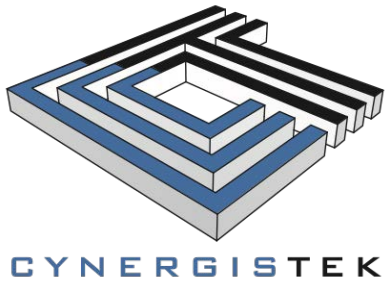
Survey

- Please take the short survey at the conclusion of the webinar



How to Prepare for an OCR HIPAA Audit

Presented by:
Mac McMillan
CEO, CynergisTek



Today's Presenter

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- CHIME, AEHIS Advisory Board
- Healthcare Most Wired Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- Top 10 Influencers in Health IT 2013
- Top 50 Leaders in Health IT 2015
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan

FHIMSS, CISM

CEO, CynergisTek, Inc.

Agenda

- Introduction
- OCR HIPAA Audit Program
- OCR HIPAA Desk Audits
- OCR HIPAA Compliance Performance Audits
- Creating An OCR Audit Toolkit
- Questions

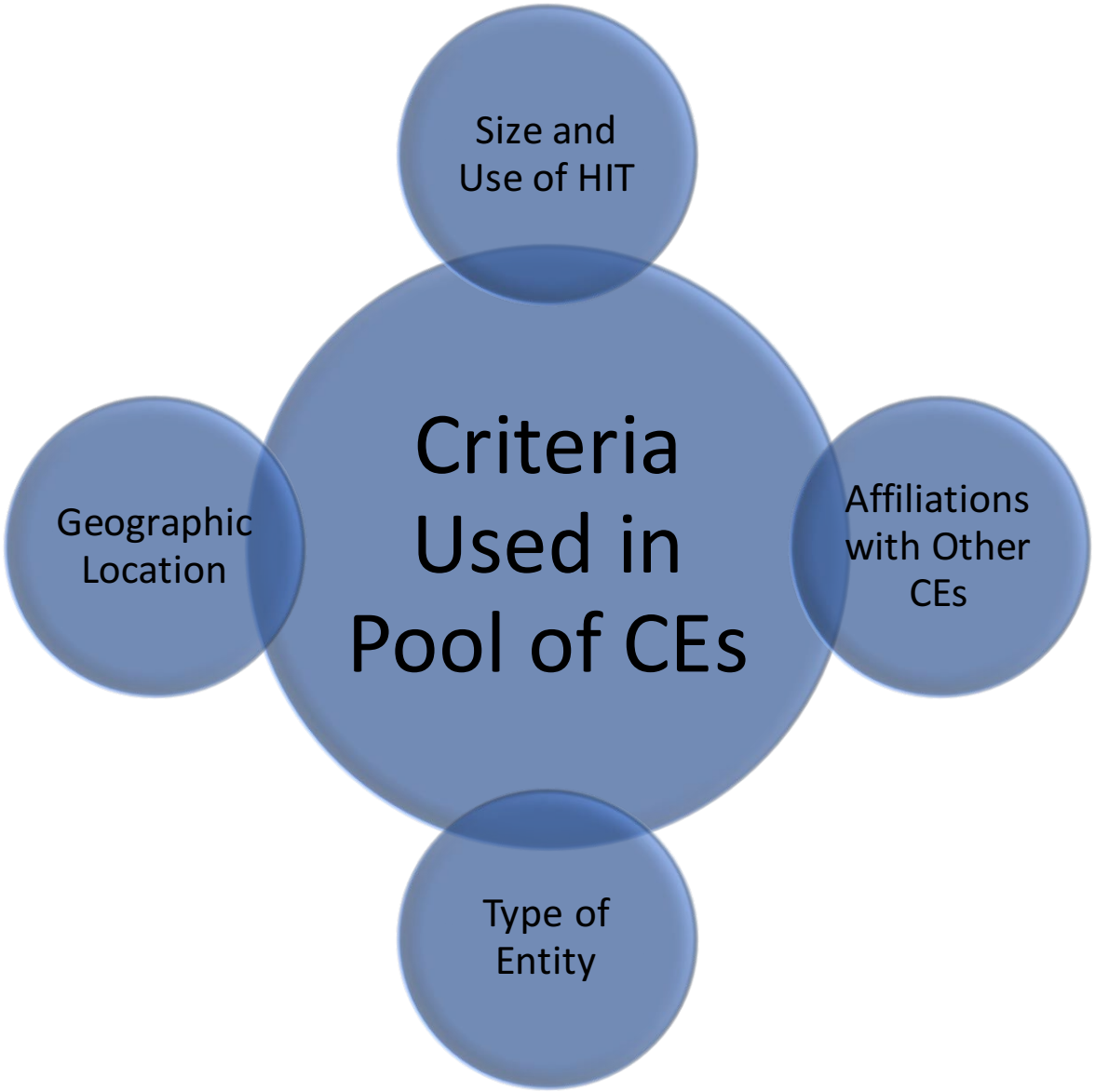
OCR HIPAA Audit Program

HIPAA/HITECH Audits

HITECH Act – Sec. 13411

- Periodic audits to ensure covered entities and business associates comply with requirements of HIPAA and HITECH
- Examine mechanisms for compliance
- Identify best practices
- Discover risks and vulnerabilities that may not have come to light through complaint investigations and compliance reviews
- Renew attention of covered entities to health information privacy and security compliance activities

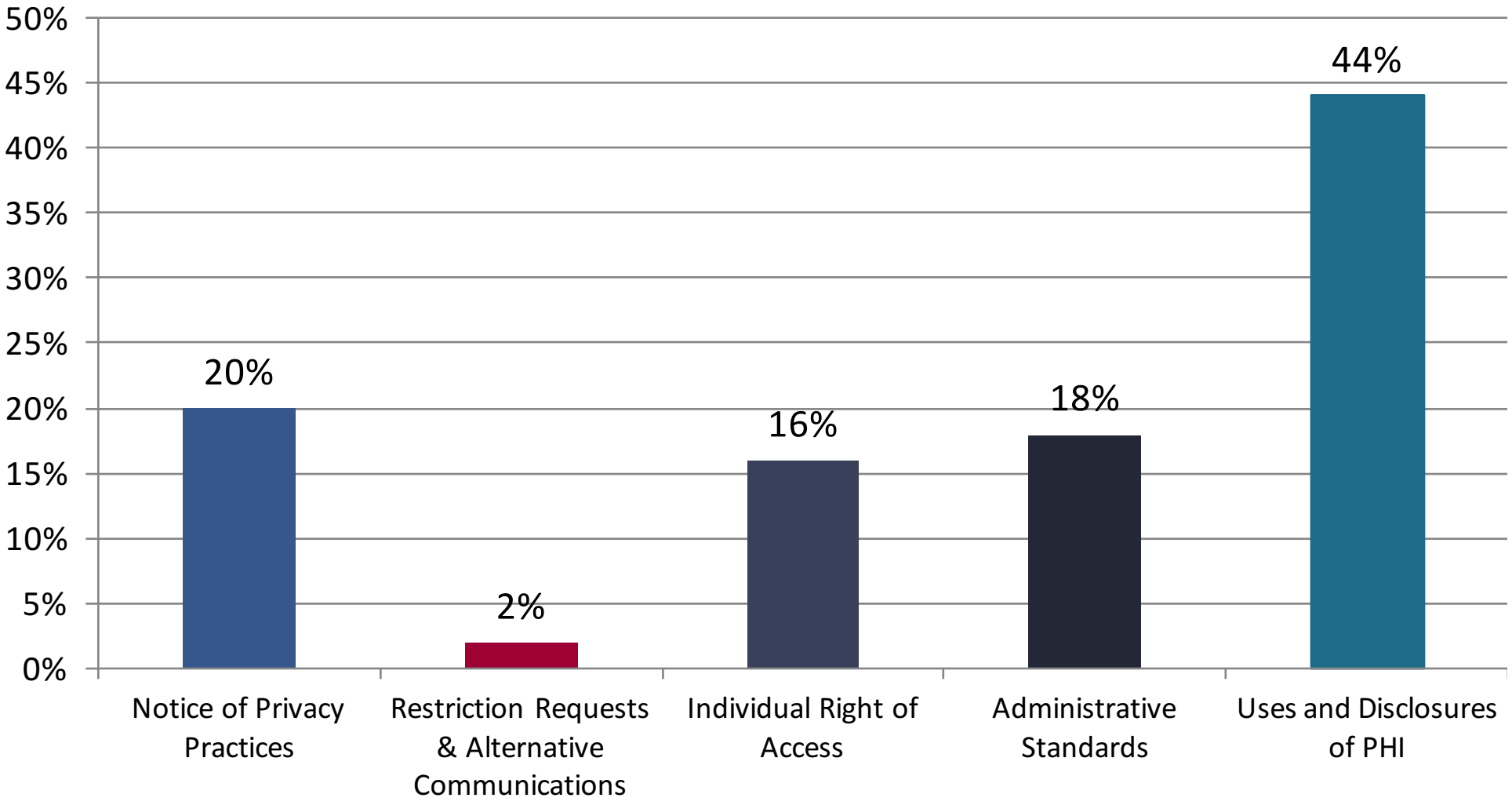
Audit Selection Criteria



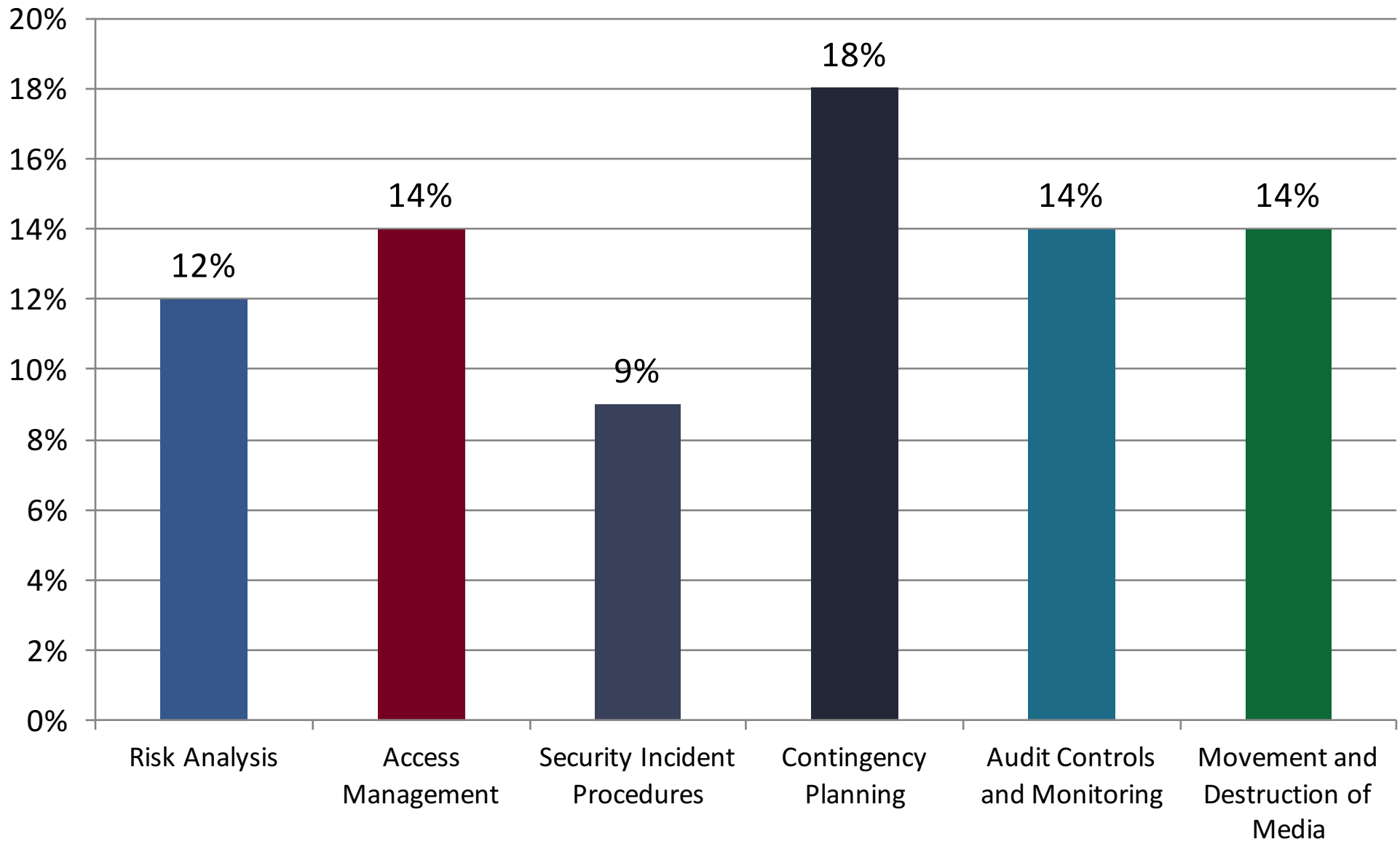
Overview of 2012 HIPAA/HITECH Audits

- On-site audits of 115 covered entities
  - 61 providers, 47 health plans, 7 clearinghouses
- No findings or observations for 13 entities (11%)
  - 2 providers, 9 health plans, 2 clearinghouses
- Total 979 audit findings and observations
  - 293 Privacy
  - 592 Security
  - 94 Breach Notification
- Percentage of Security Rule findings and observations was double what would have been expected based on protocol
- Smaller entities struggle with all three areas

Privacy Rule Findings



Security Rule Findings



OCR Desk Audit Program

OCR's Permanent Audit Program

- Permanent audit program includes desk audits and comprehensive, onsite audits
- ~200 Covered Entities to be selected for desk audits
- Equal number or less BAs selected for desk audits
- Greater number of on-site (comprehensive) audits, but no specific number given yet
- Updating audit protocol
- Audits will be performed by HHS contractors but program to be managed by OCR personnel

The Desk Audit Process

Scope of OCR Desk Audits

2015 Desk Audits of Covered Entities	• Security—Risk Analysis and risk management • Breach—Content and timeliness of breach notifications • Privacy—Notice of Privacy Practices and Access
2015 Desk Audits of Business Associates	• Security—Risk Analysis and risk management • Breach—Breach reporting to Covered Entities
2016 On-site Comprehensive Audits	• Covered Entities • Business Associates

Comprehensive Audit Process

Scope of OCR Onsite Audits

Security

- Device and media controls
- Transmission security
- Encryption of data at rest
- Facility access controls

Privacy

- Administrative and physical safeguards
- Workforce training to HIPAA policies & procedures

Other Areas

- High risk areas identified through:
  - 2015 audits
  - Breach reports submitted to OCR
  - Consumer complaints

OCR Performance Audit

On-site Audits are Performance Audits

- Conducted in accordance with Generally Accepted Government Audit Standards (GAGAS)
- Provides findings, observations, or conclusions from evaluation of evidence against established criteria
- Objective assessment of variety of attributes
  - Program effectiveness, economy, and efficiency
  - Internal controls
  - Compliance

Audit Process

Planning the Audit

- Send notification letter to the covered entity
  - Information request list
  - Entity survey
- Make initial telephone contact with Covered Entity
  - Confirm notification letter receipt
  - Respond to questions and concerns
  - Confirm due date for documentation requests

Documentation Request

OCR Random Audit Documentation Request List

Checklist Category	Document Name/Description
General Information	
General Information	Size of Covered Entity: number of employees, members or patients, facilities, EMR facility (Y/N)
HIPAA Security	
General Governance - HIPAA Security	Identify any applicable industry guidance (e.g., studies, practices, regulations, etc.) or other reference material used to develop any of the policies and procedures requested below **(No need to provide this documentation - just identify)**
General Information - HIPAA Security	Security Officer Contact Information (name, email, phone, address and admin contact info)
Administrative Safeguards	Entity-level Risk Assessment
Administrative Safeguards	Organizational chart
Administrative Safeguards	Information Security Polices, specifically those documenting security management practices and processes, such as: - Access Control - Data Protection

Preparation Work

- Conduct kick-off call
  - Confirm Covered Entity type (e.g. provider, health plan), applicable scope, audit location(s)
  - Discuss on-site visit and logistics
- Perform analysis of documentation provided by CE
  - What documents have been received and which are missing
  - Review documentation for compliance with appropriate regulatory standard or specification

On-Site Field Work

- Conduct entrance conference
  - Discuss performance audit scope, objective and approach
  - Set expectations
- Execute and document applicable audit procedures
  - Complete on-site testing
  - Conduct interviews
  - Review documentation
  - Observe appropriate facilities and workstations
- Conduct exit conference
  - Preliminary identification of compliance issues

Post Field Work

- Document results of the audit
- Finalize draft identified findings
- Issue draft performance report to CE for comment and correction
- Issue final performance audit report that includes CE comments and response

Sample Audit Protocol - Provider

Breach Notification	Privacy	Security
• Assessment for breach • Notification to individuals • Notification to Secretary • Notification to media	• Notice of Privacy Practices • Request Restrictions • Right to Access • Administrative Requirements • Amendment • Uses & Disclosures • Accounting of Disclosures	• Administrative Safeguards • Physical Safeguards • Technical Safeguards

HIPAA Security Risk Assessment

- Required element for Security Rule and Meaningful Use
- An assessment of threats and vulnerabilities to information systems that handle e-PHI
- This provides the starting point for determining what is '**appropriate**' and '**reasonable**'
- Organizations determine their own technology and administrative choices to mitigate their risks
- The risk analysis process should be ongoing and repeated as needed when the organization experiences changes in technology or operating environment

Performing a Risk Analysis

Gather Information

- Prepare inventory lists of information assets-data, hardware and software.
- Determine potential threats to information assets.
- Identify organizational and information system vulnerabilities.
- Document existing security controls and processes.
- Develop plans for targeted security controls.

Analyze Information

- Evaluate and measure risks associated with information assets.
- Rank information assets based on asset criticality and business value.
- Develop and analyze multiple potential threat scenarios.

Develop Remedial Plans

- Prioritize potential threats based on importance and criticality.
- Develop remedial plans to combat potential threat scenarios.
- Repeat risk analysis to evaluate success of remediation and when there are changes in technology or operating environment.

Creating an OCR Audit Toolkit

Building an Audit Tool Kit

- Prepare a plan to perform mock audits
- Replicate what documentation would be required under audit conditions and the timelines for production
- Use OCR's 2012 Pilot Audit Protocol
  - http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- Update the 2012 audit protocol for changes in the HIPAA Privacy, Security and Breach Notification Rules

Using the HIPAA Pilot Audit Protocol

Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Who Responsible?
Standard or implementation specification to be measured.	Plain language action to meet requirement.	Review policies and procedures and interview appropriate staff or contractors responsible for carrying out activity to meet standard or specification.	Some Security Rule Implementation Specifications provide flexibility through designating the requirement to be Addressable.	Representative Suggestions: Every org is different. Sometimes responsibilities for compliance activities are shared.

Example: Opportunity to Object

Established Performance Criteria	Key Activity	Audit Procedures	Who Responsible?
Uses/disclosures requiring opportunity for the individual to agree or to object. A health care provider must inform individual of the PHI that it may include in a directory and to whom it may disclose such information & provide the individual with the opportunity to restrict or prohibit the uses or disclosures.	Opportunity to Object to Use or Disclosure	Inquire of management as to whether objections by individuals to restrict or prohibit some or all of the uses or disclosures are obtained and maintained. Obtain and review Notice of Privacy Practices and evaluate the content in relation to the specified criteria for evidence of opportunity to object. Obtain evidence that staff have been trained to properly carry out this standard.	Privacy Officer HIM Leader Compliance Officer

Example: HIPAA Privacy Training

Established Performance Criteria	Key Activity	Audit Procedures	Who Responsible?
A covered entity must train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. §164.530(b)(2)(i)(A) Training must be provided to each member of the covered entity's workforce.	Training	Inquire of management as to whether training is provided to the entity's workforce on HIPAA Privacy Standards. Review documentation to determine if a training process is in place for HIPAA privacy standards. Review documentation to determine if a monitoring process is in place to help ensure all members of the workforce receive training on HIPAA privacy standards.	Privacy Officer HR Leader Compliance Officer

Example: Security Management Process

Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Who Responsible?
§164.308(a)(1) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the CIA of PHI held by the covered entity or business associate.	Conduct Risk Assessment	Inquire of management as to whether formal or informal policies or practices exist to conduct an accurate assessment of potential risks and vulnerabilities to the CIA of ePHI.	Required	CIO, CISO, Compliance Officer

Example: Access Controls/Encryption

Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	Who Responsible?
§164.312(a)(1): Access Control - §164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.	Encryption and decryption	Inquire of management as to whether an encryption mechanism is in place to protect ePHI. Obtain & review formal or informal policies and procedures and evaluate the content relative to the specified criteria	Addressable	CIO, CISO

Example: Notification of Breach

Established Performance Criteria	Key Activity	Audit Procedures	Who Responsible?
Notice to Individuals §164.404 (a) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Notification to Individual of Breach	Inquire of management as to whether a process exists for notifying individuals within the required time period. Obtain and review key documents that outline the process for notifying individuals of breaches.	Privacy Officer HIM Leader Compliance Officer

Iatric & CynergisTek Managed Services

Components of a Mature Audit Program

Policies

Develop and implement policies that meet the HIPAA Privacy, Security and Breach Notification Rule standards

Monitoring

Determine frequency of standard, behavioral and fraud detection monitoring

Analysis

Proactive, comprehensive auditing and monitoring that is manageable and scalable; implement ongoing analysis

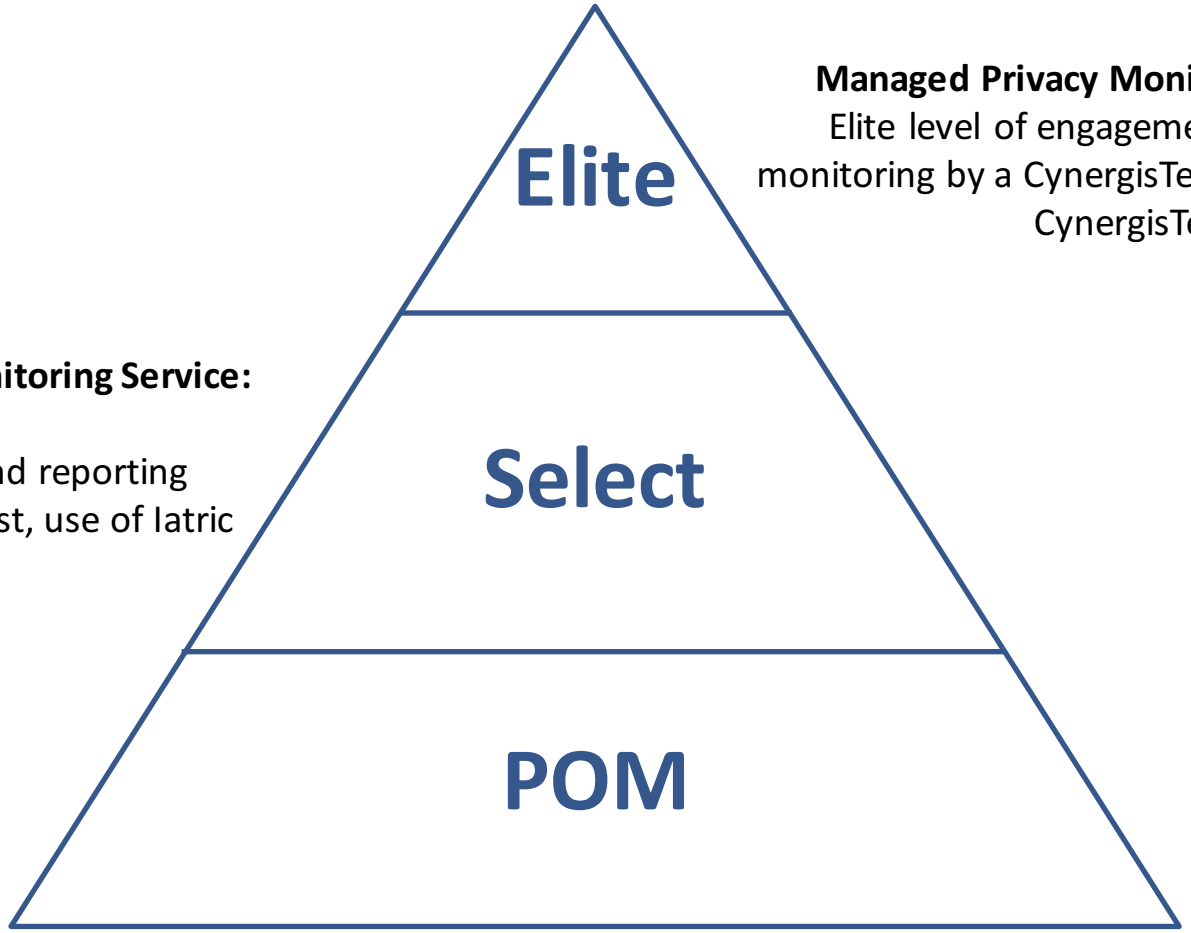
Reporting

Documentation to communicate program effectiveness, both internally and externally

CynergisTek Offers POMS

Managed Privacy Monitoring Service: Elite
Elite level of engagement, intense ongoing monitoring by a CynergisTek analyst and use of CynergisTek advisory services.

Managed Privacy Monitoring Service: Select
Ongoing monitoring and reporting by a CynergisTek analyst, use of Iatric Systems SAM solution.



Privacy Optimization Module
Proactive auditing and monitoring optimization plan. Focuses on establishing necessary processes for effective and efficient privacy monitoring.

Questions

Questions?

Mac McMillan
mac.mcmillan@cynergistek.com
512.405.8555
@mmcmillan07

How to prepare your organization for an OCR HIPAA audit

Contact Us | Survey

Survey:

Please take the survey that will appear after you leave the webinar. You could win a $100 Amazon.com Gift Card.

Follow Us:

http://new.iatric.com/blog-home

For more information:

Please contact your **Iatric Systems Account Manager**
Send an email to **info@iatric.com**

Thank you for attending!

IATRIC systems