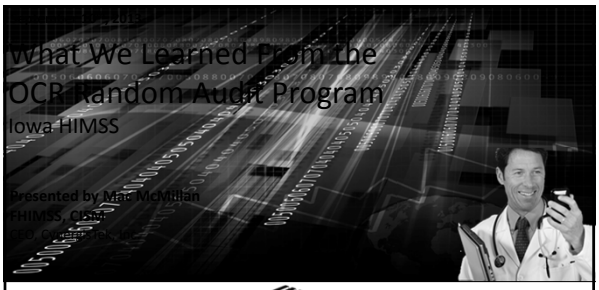
What We Learned From the OCR Random Audit Program

Iowa HIMSS

Presented by Mac McMillan
FHIMSS, CISM
CEO, CynergisTek, Inc.



CYNERGISTEK

www.cynergistek.com

Today's Presenter

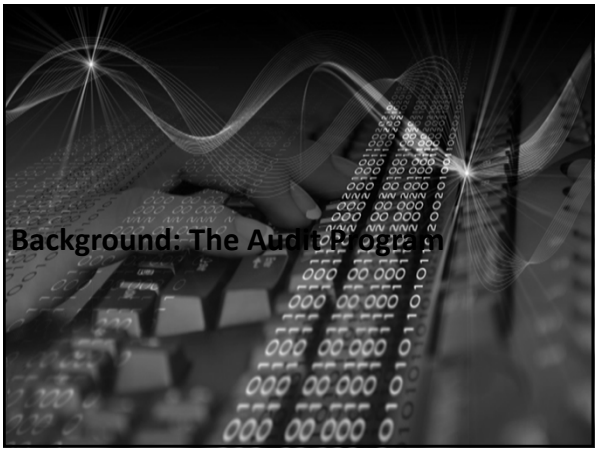
- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- Chair, HIMSS P&S Steering Committee
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- HealthTech Industry Advisory Board
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
FHIMSS/CISM
CEO CynergisTek, Inc.

Inside an OCR Audit

Agenda

- The Program
- The Audit Process
- The Audit Protocol
- Lessons Learned
- Questions



HITECH: Establishes Requirement

- The American Recovery & Reinvestment Act 2009, in Section 13411, requires HHS to conduct periodic audits to ensure covered entities and business associates are meeting HIPAA compliance requirements
- To begin this audit process HHS launches pilot program
- The OCR Random Audit Program commenced FY 2012 and initial audits were completed CY 2012

Categories

Level 1 Entities
- Large Provider / Health Plan
- Extensive use of HIT - complicated HIT enabled clinical /business work streams
- Revenues and or assets greater than $1 billion

Level 2 Entities
- Large regional hospital system (3-10 hospitals/region) / Regional Insurance Company
- Paper and HIT enabled work flows
- Revenues and or assets between $300 million and $1 billion

Level 3 Entities
- Community hospitals, outpatient surgery, regional pharmacy / All Self-Insured entities that don't adjudicate their claims
- Some but not extensive use of HIT – mostly paper based workflows
- Revenues between $50 million and $300 million

Level 4 Entities
- Small Providers (10 to 50 Provider Practices, Community or rural pharmacy)
- Little to no use of HIT – almost exclusively paper based workflows
- Revenues less than $50 million

Entities Selected

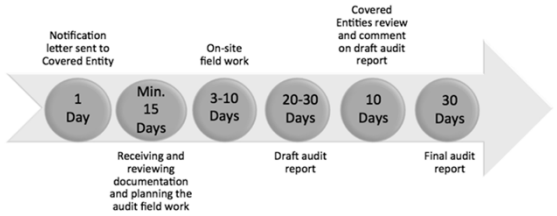
	Level 1	Level 2	Level 3	Level 4	Total
Health Plans	13	12	11	11	47
Healthcare Providers	11	16	10	24	61
Healthcare Clearinghouses	2	3	1	1	7
Total	**26**	**31**	**22**	**36**	**115**

A Dynamic Program

- Pilot year of program ended December 2012
- Results of 115 audits studied to develop recommendations
- Conducting survey of auditees to receive feedback
- Process, Protocol and reporting have changed multiple times
- Expect more change…

The Audit Process

The Audit Timeline



Notification

- Phone call to confirm name and address for letter.
- Notification by registered mail 30 – 90 days in advance. Includes letter from OCR providing basis for audit under HITECH and introduces the audit process.
- The letter is addressed to the CEO so organizations need to redirect it as soon as it arrives.
- Follow up call to confirm receipt.
- Timing for audit activities tied to date organization receipts for letter.

Submit Documentation

- List of documents is provided at attachment to the Notification letter.
- List of items such as policies, procedures, plans, assessments, demographic information, forms, etc.
- Information is due within **15** business days of receipt of the Notification letter.
- Important to provide as much as possible.

On-Site Data Collection

- On-site field activities can begin 20 – 60 days from notification.
- On-site data collection can last from 3 – 10 business days and involve up to 5 auditors.
- The on-site visit will include interviews of key personnel, other staff members, site walkthroughs, operational reviews, and requests for further information.
- On-site activities will include entrance/exit conferences.
- General focus for audit is provided, but audits are not scripted.

Post On-Site Activity

- The Audit team will take 20 – 30 days following the on-site visit to produce a draft report.
- The site can expect additional questions/requests for information while the report is being written.
- Report will include a Letter of Representation, spreadsheet with list of findings/observations.
- Upon completion the draft report is provided to the site. It includes site information, findings/observations, recommendations, and request for response.

Draft Report & Response

- The site has 10 business days from the date of receipt of the report to review and provide a response to deficiencies noted.
- Site should review the report closely, identify clarifying questions, mitigating information, and plans for remediation.
- Site should take full advantage of expert advise from consultants and legal when developing response.

Final Report & Disposition

- Auditors have up to 30 days to finalize report.
- Final report and site responses forwarded to OCR.
- OCR determines final disposition, provides report to audited entity.
- OCR reserves the right to conduct follow up review or investigate where circumstances warrant.

The Audit Protocol

Audit Procedures

- Current # 169 procedures
- Broken down into Key Activities and requirements
- Guide the audit process/don't dictate
- hhs.gov/ocr

Example Audit Procedure

- **Inquire** of management…
- **Obtain** and review policies and procedures…
- Obtain and **review evidence/documentation**…
- If CE has chosen not to fully implement, then must have **documentation of why**…

Readiness Tool

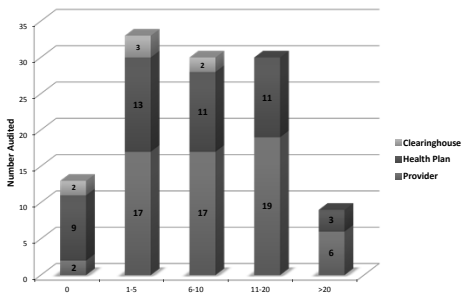
- Understand how Protocol works
- Use as tool to conduct "spot" audits
- Exercise fully demonstration of tasks
- Produce documentation

Lessons Learned

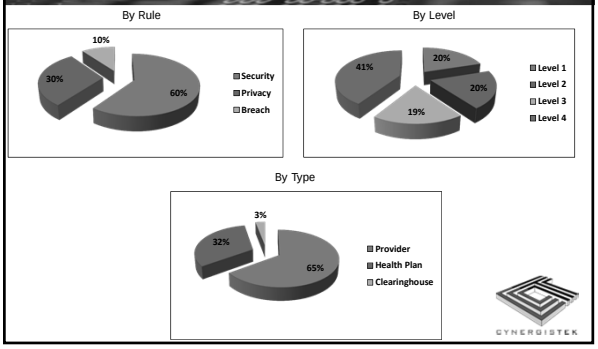
Interesting Observations

- 10% of selectees had no audit findings, 10% of selectees were totally unprepared for audit
- Three common denominators told the story: size, providers & security
- Significantly fewer findings for those entities who fully implemented addressable specifications
- Most common excuse heard for non-compliance – "unaware of the requirement"
- Other reasons for findings: Lack of application of sufficient resources, incomplete implementation and complete disregard

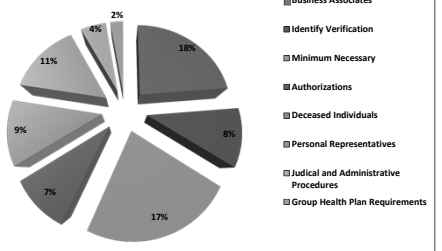
Overall Outcomes



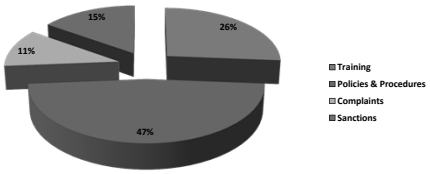
Lessons Learned Overall



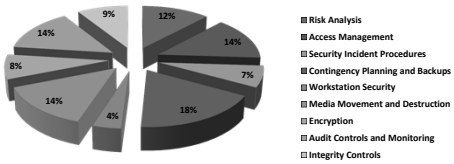
Privacy Outcomes by Issue



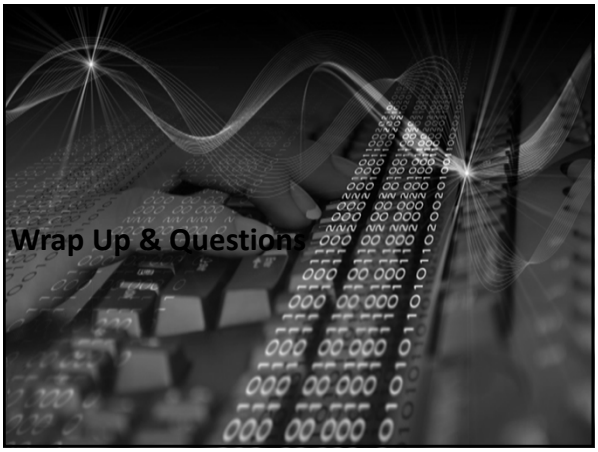
Privacy Outcomes by Function



Security Outcomes by Issue



Wrap Up & Questions



What's Next

- OCR is completing its audit program evaluation, all elements; process, protocol, reporting
- OCR has requested feedback from audited organizations
- OCR considering creating webpage on OCR site for identifying best practices
- Develop technical assistance for industry based on results of audits
- Determine where follow up is appropriate

Thank You

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555
www.cynergistek.com