



ARRA & HITECH

Why Auditors and Security Professionals
Should Care

ISACA North Texas Chapter
February 11, 2010

Austin Hutton CISA, CISM, CGEIT
Greater Yield



Who is Greater Yield?

Greater Yield is a management consulting company focused on providing the “right information at the right time”.

Our primary focus is on operational and technical assessments regarding strategic alignment, operational efficiency, risk assessment, compliance management and technology governance.

Our specialty focus on health care IT is targeted to providing readiness and planning assessments that encompass strategic, financial, technical, and operational evaluations to healthcare organizations.

Objectives and Agenda



Discussion Objectives:

- Implications of new federal legislation on health care practices
- Impact to organizations with protected health information
- Opportunities for IS auditors and Information Security managers

Agenda:

- Overview of ARRA/HITEC Act components
- Review the issues and understand the increase in information risk
- Understand the opportunities for CISA and CISM practitioners

Acronyms



Acronym	Description / Definition
CE	Covered Entity is typically a hospital, doctor, employer or anyone who keeps and uses Protected Health Information and is regulated by HIPAA
BA	Business Associate, someone who contracts with an CE for services, i.e. legal, accounting, marketing, etc.
HHS	Department of Health and Human Services
EHR	Electronic Health Record
EMR	Electronic Medical Record
CPOE	Computerized Physician Order Entry
PHI	Protected Health Information
CCHIT	Certification Commission for Healthcare Information Technology
PM	Practice Management typically refers to basic practice automation software

ARRA & HITECH



- **ARRA**
 - The **American Recovery and Reinvestment Act of 2009**, is an economic stimulus package enacted February 2009. ARRA, along with similar economic recovery legislation passed in late 2008, includes the Economic Stimulus Act of 2008, the Emergency Economic Stabilization Act of 2008 and the Troubled Assets Relief Program (TARP).
- **HITECH**
 - **Health Information Technology for Economic and Clinical Health (HITECH) Act** is included in ARRA legislation. The main goal of the HITECH Act is to encourage the adoption of electronic health records (EHRs) through incentive payments to physicians. HITECH also includes several significant changes to HIPAA regulations.

2/3/10

greater>yield], ltd. CONFIDENTIAL

5

HITECH Act - Overview



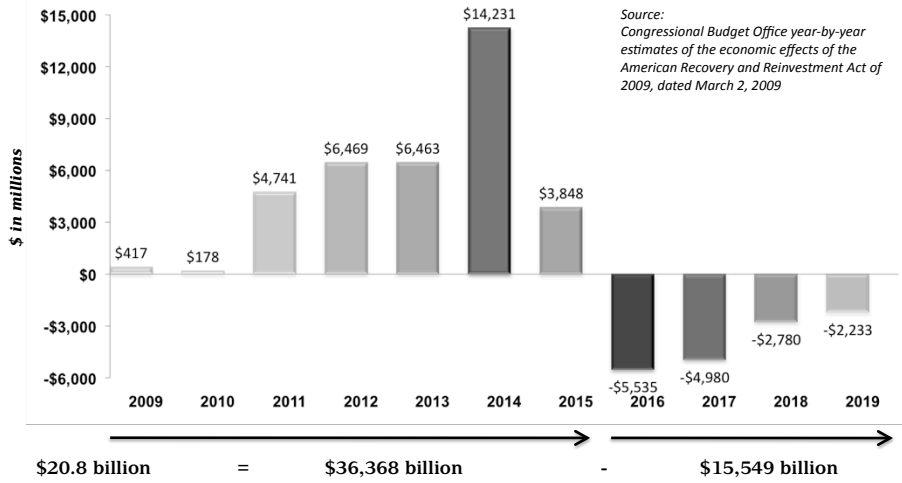
- **Significant financial incentives for adoption of EHR**
 - Includes “Jump Start” funding for some research activities
 - Incentive payments available beginning in 2011 - \$ 44,000 per physician
 - Penalty provisions begin in 2015 – reduced Medicare payments
- **Creates/expands Health Care IT agencies and committees**
 - Health Information Technology Policy Committee (HIT Policy Committee)
 - Health Information Technology Standards Committee (HIT Standards Committee)
 - Sets standards for “Meaningful Use” and “Certified” applications
- **Substantially expanded the HIPAA Privacy/ Security Rules**
 - Increased penalties for HIPAA violations
 - Expands enforcement scope Office of Civil Right, FTC and state AG’s
 - Requires mandatory data security breach reporting

2/3/10

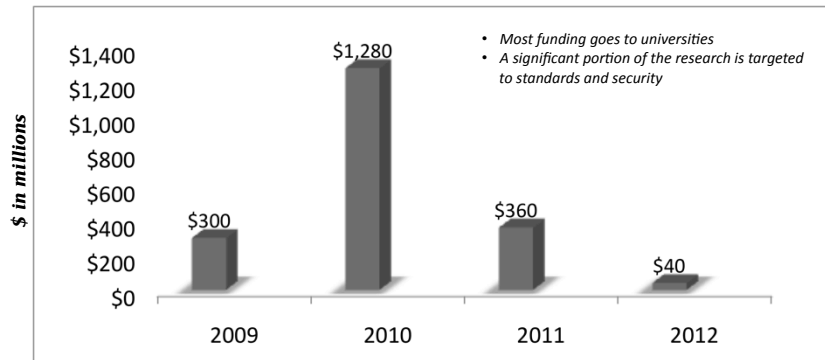
greater>yield], ltd. CONFIDENTIAL

6

HITECH Funding for Implementation of EHRs (Medicare and Medicaid Incentive Payments)



HITECH - Jump-Start Funding



Meaningful Use



- Requirements for Incentive Payments
 - The EHR participant must be a “meaningful EHR user”
- “Meaningful Use” will be met in the reporting period if:
 - EHR technology is used in a “meaningful” manner
 - “Meaningful Use” involves using a “certified” EHR vendor in a way that allows the electronic exchange of health information to improve the quality of health care
 - The applicant must also submit clinical quality and other metrics in order to qualify
- “Meaningful Use” is a “Phased” approach
 - To receive first year payments applicant must demonstrate that they have adopted, implemented or upgraded a “certified” EHR technology
 - Three defined phases progressively increase the use of “certified” EHR technology by providing improved electronic communication of health records, improved patient practices and improved quality and efficiency

2/3/10

greater>yield], ltd. CONFIDENTIAL

9

Certified Software



- “Certified” EHR software demonstrates compliance with the Act requirements and inter-operability
- To receive incentive maximum payments “certified” software is required
 - CCHIT certifies EHR systems, expect other certifying agencies
 - Only a handful of vendors today meet the ‘new’ criteria
 - Current standards apply primarily to discrete applications and focus mostly on data standardization and inter-operability
 - Most of the ‘new’ effort is meeting QA, inter-operability and scope of service criteria
 - “Certifications” operate on 2-year cycles
- Hundreds of vendors today covering multiple aspects of healthcare
 - Vendor attrition and consolidation is likely
 - Multiple service models are being offered
 - Stand alone, SaaS, Full Outsourcing

2/3/10

greater>yield], ltd. CONFIDENTIAL

10

Change to HIPAA Rules



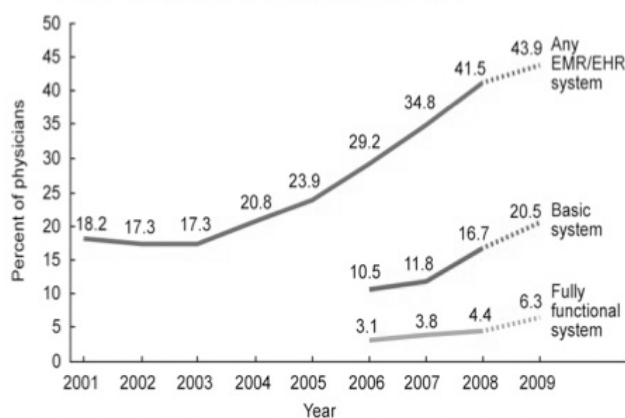
- Enforcement expanded to Office of Civil Rights, Federal Trade Commission and state Attorneys' General
- Penalties are more rigorous
 - “Willful neglect” and non-corrected violations start at \$50,000 per violation and go to \$1.5MM per violation with no cap
- Patient requests NOT to share information must be honored
 - Patients may request copies of any information sharing
- Further limits how PHI may be shared with “Business Associates”
- Business Associates are now directly accountable under HIPAA
- Covered entities and Business Associates are required to notify of *unsecured* data breaches affecting more than 500 people
 - Notifications must go to affected patients, HHS and the media
 - Effectively, HITECH implements a federal data breach law

2/3/10

greater>yield], ltd. CONFIDENTIAL

11

How Will The Industry React?



➤ CDC forecasts a low rate of adoption for full function systems

➤ Industry analysts have long predicted that significant adoption would require financial incentives

➤ HITECH is intended to aggressively increase the rate of EHR adoption

CDC/National Center for Health Statistics

2/3/10

greater>yield], ltd. CONFIDENTIAL

12

Is The Industry Prepared?



Results from a recent study* – HITECH Act compliance

- 53% of Covered Entities were generally or barely aware of compliance actions needed
- 68% of Business Associates were generally or barely aware of compliance actions needed
- Prior to HITECH Privacy and Security programs lagged
 - Only 43% of Business Associates had a privacy compliance program
 - Only 26% of Business Associates had a security compliance program
 - Over ½ of all respondents acknowledged deficiencies in HIPAA compliance
- The problem is dramatically worse in smaller organizations
- Management commitment and budget are key limitations

* Ponemon Institute Study November 2009

2/3/10

greater>yield], ltd. CONFIDENTIAL

13

Other Issues Are Surfacing



- HHS advisory panel expresses concerns over the lack of risk assessments
- Congressional Report highlights several IT/management issues
 - IT and enterprise strategy disconnected
 - Lack of CEO champions
 - Rush to implement and capture incentives
 - Limited information technology, security, and risk resources
 - Immature process analysis and documentation
 - Paper based quality metrics
 - Limited program/project management experience
- Multiple new technology options create unintended consequences
 - Financial implications of implementations not well understood.
 - Contract oversights
 - Technical models not fully understood
 - Ongoing resource requirements overlooked

2/3/10

greater>yield], ltd. CONFIDENTIAL

14

General Implications



- Demand for IT workers in health care is increasing
 - The industry is short 50,000 to 75,000 Health IT workers to support electronic health care systems
 - \$80M in funding has been established for health care IT training programs
- Industry experts are calling for more expert third-party involvement, specifically IS auditors and information security specialists
 - CISA/CISM will benefit from the increased demand
- Major consultancies are ramping up health care initiatives
- Major focus by software vendors will increase demand for IT expertise in audit and information security management
- Increased demand will ramp up rather quickly over the next two years
 - Broad based growth across multiple sectors, not as dramatic as SOX

2/3/10

greater>yield], ltd. CONFIDENTIAL

15

Implications for CISA



- IS audit for healthcare will expand as the scope and complexity
 - Growth will be in smaller health care facilities
 - Tremendous growth in Business Associate exposures
- Consultative roles will increase
 - Evaluation of health care systems vendors
 - Skills, infrastructure, contract implications
 - Technical assessments – ‘as is’, ‘to be’, ‘what if’
 - Compliance reviews – current employers, Business Associates
- Updating, creating and conducting IS audit programs
 - General controls, application controls, database controls, etc
 - Updating, creating, and conducting HIPAA audits
 - Third-party arrangements
 - Assess the current security and privacy programs

2/3/10

greater>yield], ltd. CONFIDENTIAL

16

Implications for CISM



- Risk assessments are identified as a critical success factor
 - Specifically identified gap in congressional and HHS hearings
 - Shortage of expertise in the industry
- Overall Information Security assessments is a critical requirement to comply with HIPAA rule changes
 - Implications for Business Associate relationships
 - Reassessing risk profiles
 - Assessing breach identification and notification capabilities
 - Establishing ongoing privacy and security priorities
- Increasing visibility in consultative roles
 - Contract reviews with vendors and business associates
 - Assessment of document retention/management risks
 - Assessment of business continuity and disaster recovery plans

2/3/10

greater>yield], ltd. CONFIDENTIAL

17

Reference Sources



- www.ehrdecisions.com
- www.govhealthit.com
- www.healthit.hhs.gov
- www.healthcareitnews.com
- www.informationweek.com/healthcare/
- www.ponemon.org/research-studies-white-papers
- Current ISACA Journal – Performing a Risk Assessment

2/3/10

greater>yield], ltd. CONFIDENTIAL

18

Contact



Austin Hutton *CISA, CISM, CGEIT*
wahutton@greateryield.com
Cell: 972-567-9875