Security and the new HITECH ACT regulations: Is your registry ready?

Iris Zachary, MS
Missouri Cancer Registry
MU Informatics Institute

Presenter Disclosures

Iris Zachary

(1) The following personal financial relationships with commercial interests relevant to this presentation existed during the past 12 months:

No relationships to disclose

Overview

- ARRA American Recovery and Reinvestment Act of 2009
- HITECH Act/ MO-HITECH Act
- HIPPA
- Implications for Central Cancer Registries

ARRA (Public Law 111-5)

- American Recovery Reinvestment Act (ARRA) and Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Stimulus Law was signed February 17, 2009
- HITECH: Title XIII of ARRA was given a subtitle: Health Information Technology for Economic and Clinical health Act (HITECH).

ARRA & HITECH Funding

- ARRA
  - $787 Billion federal stimulus package passed by Congress and signed by Obama in February 2009
- HITECH Act
  - $50 billion section of the stimulus package focused on funding and supporting widespread adoption of health information technology
  - $19.2 billion in spending on health IT
- MO-HITECH
  - $1 billion funding opportunity for Missouri over the next five years http://www.slideshare.net/learfield/mohitech-presentation

HITECH Act in effect: Implications for healthcare

- Incentives for adoption of EHRs
- Health Information Exchange (HIE)
- New privacy regulation

  (Subpart D of XIII) for HIPPA and non-HIPPA entities
- HI and HIT opportunities

HIPAA Security Enforcement: How HITECH has expanded HIPAA requirements

- Breach
  - – Determine if the breach involved PHI
  - – Breach of PHI (unauthorized)
  - – Does safe harbor apply
- Safe Harbor
  - – Notification is required for breach of unsecured PHI
  - – Two methods to secure PHI are encryption and destruction

HIPAA Security Enforcement: How HITECH has expanded HIPAA requirements contd

- Covered entities
  - – Be prepared to investigate the breach
  - – Provide a root cause analysis of the breach

    Document all your security issues / potential breaches
- Key number is 500
- Common issues:
  - – Access control and management
  - – Security awareness training and incident procedures
  - – Devices and media control

Expanded security rules that apply to CCRs

- Access control and Management
  - – NIST security checklist for remotely accessed PII or physically transported PII

    (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf)
- Devices and media control
  - – Encryption of all mobile devices
  - – No PII on mobile devices
- Security awareness training and incident procedures
  - – Documentation (Breach)

Central Cancer Registry

- HIPAA (1996) Health Insurance Portability and Accountability Act
  - – Security and Privacy
- OMB Protection of Sensitive Agency Information Memorandum
  - – Encrypt all data on mobile computers/devices
  - – Allow remote access only with two-factor authentication
  - – Use a time-out function for remote access
  - – Log all computer-readable data extracts from Databases that are holding sensitive information
- ARRA - HITECH (2009)
  - – Expanded security, privacy and breech guidelines

Central Cancer Registries Security Standards

- –NAACCR Standards
  - Structural requirements
  - Registry policies and procedures
  - Data use and release
  - Information technology policy and procedures
  - Disaster recovery
- –Federal Guidelines
  - VHA directive

Implications for CCRs – cont'd

- Assess security
  - – Security audit
- Develop an action plan
  - – Timelines
  - – Develop Security Team
  - – Develop Security Plan
- Key recommendations/ Security Plan
  - – Rethink and redo and restructure

Steps

- Security Team
  - Build your security team with a breach team subgroup
  - Develop your security plan
  - Start with a security assessment
  - Audit

Steps - cont'd

- Encryption
- Assess your software and hardware
  - Invest in state of the art equipment and security devices (mobile devices)
- Data storage and transmission
- Backups
- Include encryption procedures in your daily routine and training

Steps – cont'd

- Compliance with Security Requirements
  - Restructure and refine routines compliant with the new security requirements
  - Develop and incorporate security training for all employees
  - Extend your lessons learned to your business partners

Steps – cont'd

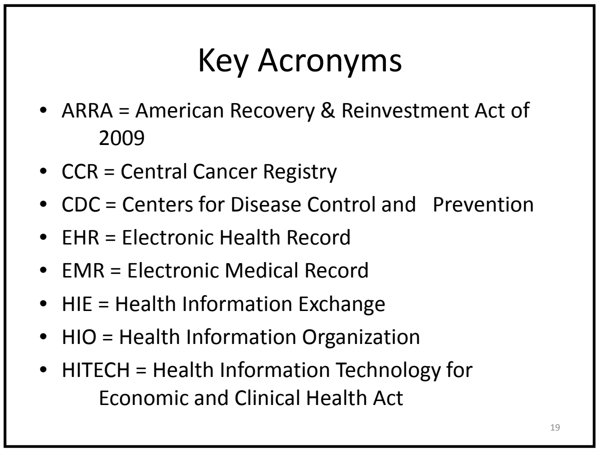
- Adapted applications
- Develop educational material
- Conduct training sessions
- Make resources available for reporting facilities

What it all means

- More audits
- Enforcement
- Tougher fines
- Accountability
- Copies of records
- "Minimum necessary" disclosures
- Marketing restrictions

Conclusion

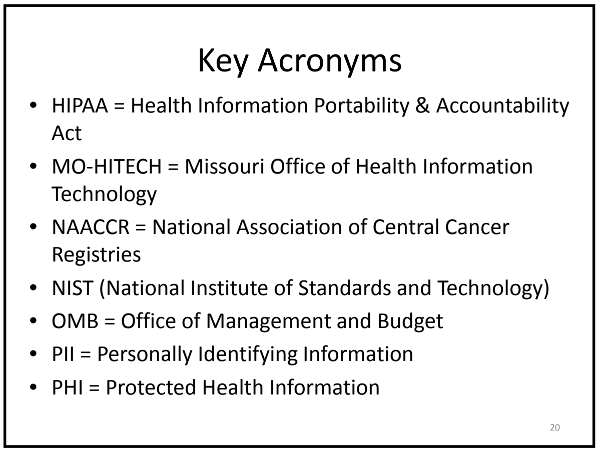
- CCRs are established data repositories with a history in security and confidentiality
  - Expand security measures and become leaders in HITECH compliance
- CCRs are an effective and efficient data source for a wide range of public health research priorities
  - Reducing cancer disparities in cancer detection
  - Prevention and treatment
  - Surveillance



Key Acronyms

- ARRA = American Recovery & Reinvestment Act of 2009
- CCR = Central Cancer Registry
- CDC = Centers for Disease Control and Prevention
- EHR = Electronic Health Record
- EMR = Electronic Medical Record
- HIE = Health Information Exchange
- HIO = Health Information Organization
- HITECH = Health Information Technology for Economic and Clinical Health Act

19



Key Acronyms

- HIPAA = Health Information Portability & Accountability Act
- MO-HITECH = Missouri Office of Health Information Technology
- NAACCR = National Association of Central Cancer Registries
- NIST (National Institute of Standards and Technology)
- OMB = Office of Management and Budget
- PII = Personally Identifying Information
- PHI = Protected Health Information

20