Central Cancer Registry Security
ARRA HITECH: Challenges, Opportunities and Implications

NAACCR 2011
Louisville, KY
Iris Zachary, MS
Doctoral Candidate MUII
Nancy Cole, BS, Jeannette Jackson-Thompson, PhD, MSPH
Missouri Cancer Registry and Research Center
Department of Health Management & Informatics
University of Missouri Informatics Institute
University of Missouri, Columbia, MO

MCR is supported in part by a cooperative agreement between the CDC and the Missouri Department of Health and Senior Services (DHSS) (#U58/DP000820-03) and a Surveillance Contract between DHSS and the University of Missouri.
Overview

- Background
  - HIPPA, HITECH, ARRA
  - What is new for CCRs

- Security Issues
  - Opportunities
  - Challenges - Physical Security
  - Electronic Security
  - Disaster/ Backup

- Security Procedures
  - Implications - Awareness
  - Education
  - Increase Security
To ensure Missouri Cancer Registry and Research Center MCR-ARC compliance with new and existing security regulations and standards
- HIPPA effective 1996
- HITECH ACT interim final rule 2009 effective 2010

Refer to the original bill:
- ARRA, H.R. 1
- TITLE XIII: Health Information Technology.
- Within the HITECH Act, the Privacy and Security provisions are contained in: TITLE XII: Health Information Technology, Subtitle D, Privacy
What is new that applies to CCRs

- HITECH increased Privacy and Security requirements
- Enforcement of requirements - stronger
- Business Associates must comply with same requirements then Covered Entities
- Security Provisions - stronger and clarified
- Privacy Provisions - stronger and clarified
For CCRs ...

- HITECH increased Privacy and Security Requirements
  - Breach and Safe Harbor
    - Determine if the breach involved PHI (unauthorized)
    - Does safe harbor apply (encrypted PHI)
  - Privacy and Security Breach Notifications to Individuals
    - No later than 60 days after discovery
    - for >500 /report to HHS
  - Safe Harbor
    - Notification required for breach of unsecured PHI
    - Encrypt or delete data at rest
    - Encrypt all data transmissions
Business Associates of HIPAA Covered Entities must comply with the Security Rule and Privacy Rule

- Business Associates
  - Business Associates must report privacy and security breaches to Covered Entity
  - Subject to same civil and criminal penalties as Covered Entities

- Personal Health Record Vendors – Now Covered
  - Vendors must report if there was a security breach
- Data breaches must be reported (maintain a log)
- New Penalties defined
  - Fines range from $100 to $50000 for each violation
Safeguards

- Administrative
  - Policy and Procedures for PHI
  - Disciplinary Actions Policy
  - Security Officer, Privacy Officer

- Technical
  - Encryption of PHI
  - Access Control

- Physical
  - Workstation Security
  - Facility Access Control
Elements of Security overlap with Privacy

- The HIPAA Security Rule only covers PHI in electronic form (EPHI)
- Privacy rule requires training for all staff in contact with PHI
- Policy & Procedures need to include HIPPA and HITECH requirements
- PHI transmitted by fax or telephone is covered by the HIPAA Privacy rule
Opportunities

- Missouri Cancer Registry
  - Security Audit
    (http://mcr.umh.edu/mcr-presentations-2.html)
  - Complete review of physical and electronic workspace
  - Assessment through the MU’s security team
  - Training through the MU’s security team
Actions Steps

- Risk assessment and analysis
  - What is your risk?
  - What safeguards are in place?
    http://infosec.missouri.edu/pdf/wism-form.pdf
- Updated Policy & Procedures
- Review of all Business Associates
- Review of your environment (every 2 years)
This is how we started 2005
Challenges - Security Issues

- Physical Security
  - Location of all computers
  - Require name tags (large departments)
  - Who has keys to the work area?
  - Are fax and printers in a secure area?
  - Are file cabinets with PHI locked?
200 Breaches Impacting Almost 5.9 Million Individuals, with Theft and Loss of Laptops and PEDs Major Cause (December 2, 2010.M) on its Web site

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Full Data Set: CSV format (18 KB) XML format (57 KB)

Select a column head to sort by that column. Select again to reverse the sort order. Select an individual record to display it in full below the table.

<table>
<thead>
<tr>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Individuals Affected</th>
<th>Date of Breach</th>
<th>Type of Breach</th>
<th>Location of Breach Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnitedHealth Group--SAEC</td>
<td>MN</td>
<td>1,270</td>
<td>2010-07-08</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper Records</td>
</tr>
<tr>
<td>Ashley and Gray DDS</td>
<td>MO</td>
<td>9,209</td>
<td>2010-01-10</td>
<td>Theft</td>
<td>Desktop Computer</td>
</tr>
<tr>
<td>University of Missouri Health Plan</td>
<td>MO</td>
<td>769</td>
<td>2011-01-10</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper</td>
</tr>
<tr>
<td>Union Security Insurance Company</td>
<td>MO</td>
<td>820</td>
<td>2011-03-24</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>Robert Wheelerly, DDS, PC</td>
<td>MO</td>
<td>1,400</td>
<td>2010-10-17</td>
<td>Theft</td>
<td>Laptop</td>
</tr>
<tr>
<td>Mid America Kidney Stone Association, LLC</td>
<td>MO</td>
<td>1,000</td>
<td>2009-09-22</td>
<td>Theft</td>
<td>Network Server</td>
</tr>
<tr>
<td>Union Security Insurance Company</td>
<td>MO</td>
<td>935</td>
<td>2011-02-18</td>
<td>Unauthorized Access/ Disclosure</td>
<td>Other</td>
</tr>
</tbody>
</table>
Security Issues

- Technical Security
  - Remote access
  - Electronic file transfer of PHI
  - Are you in compliance with your departments security regulations and requirements at your institution?
  - Do you make security training and awareness available to your employees?
  - Policy and Procedure manuals should have a section on security for your environment
Hippa.com
Nearly 8.3 Million Individuals Impacted by 249 Privacy and Security Breaches Reported by HHS;
More Training on Safeguarding PHI Required

Ed Jones [20110318]
http://www.hipaa.com/2011/03/
Nearly 8.3 Million Individuals Impacted by 249 Privacy and Security Breaches Reported by HHS; More Training on Safeguarding PHI Required

The HHS Office for Civil Rights (OCR), which is responsible for privacy and security enforcement under the Health Insurance Portability and Accountability Act (HIPAA) and HITECH Act provisions that strengthened privacy and security enforcement, is required to post those breaches on its Web site. As of March 17, 2011, OCR had posted on its Web site 249 breaches that had impacted 8,289,236 individuals reported by covered entities. With regard to the 177 privacy and security breaches involving electronic PHI, 104, or approximately 59%, involved laptops and portable electronic devices (PEDs)—not otherwise identified. All but 4 of these reported breaches of laptops and PEDs involved theft or loss. These breaches should not be occurring! Covered entities and business associates should be encrypting their electronic PHI on portable and mobile devices. Clearly, they should be emphasizing safeguard policies and procedures such as encryption of electronic PHI, and initiating a meaningful training program for workforce members on “awareness and understanding” of and abiding by those policies and procedures.
Security Issues

- Administrative Security
  - Disaster
    - Katrina, LA
    - Joplin, MO
  - Backup Security
    - Where is your data?
    - Request a full backup from your off site location regularly (every 6 months)
Implications - Security Procedures

- Awareness
  - Assessment
  - Provide service
- Checklist
  - Administrative
  - Technical
  - Physical
- Education
  - Training
  - Provide service
Checklist

- Two methods for data at rest: encrypt or destroy PHI
- All mobile devices must be encrypted
- Dispose of any PHI properly (shred)
- Dispose of digital media containing PHI (shred/destroy/erase)
- Any PHI on paper needs to be locked up when unattended
- Every computer (laptops) must have a password-protected login
- Your login should time out after inactivity, lock your PC if you leave
- No PHI in email including internal emails
- Educate employees and Business Associates
- Breach Team
- Include the new requirements into your Policy and Procedures with specific guidelines and action steps
- 60 days notice to report a breach for covered entities and business associates
- >500 report needs to be made to HHS
- Covered Entities must maintain log of data security breaches - annual submission to HHS
- Business Associates report breach to the covered entity, the covered entity notifies individuals
Result

- **Achieve greater Security and Compliance**
  - Identify vulnerabilities
  - Consider internal and external security breaches

- **Increase Awareness**
  - Education internal and external including your Business Associates
  - Clear expectations and guidelines for employees and Business Associates
Even in a safe environment improvements can be made to security policies and procedures

Don’t stop looking at your workplace - security is not a finished product, it is an ongoing process

Security breaches by employees do occur - expect the unexpected
Questions?

zacharyi@missouri.edu