SECURITY ISN’T JUST A CENTRAL CANCER REGISTRY ISSUE:

HOW ONE CCR HELPED REPORTING FACILITIES IMPROVE SECURITY

NAACCR 2011 LOUISVILLE, KY
Nancy Cole, BS, CTR \textsuperscript{1,2}

Iris Zachary, MS, CTR, Doctoral Candidate \textsuperscript{1,2,3}

J. Jackson-Thompson, PhD, MSPH \textsuperscript{1,2,3}

\textsuperscript{1} Missouri Cancer Registry and Research Center
\textsuperscript{2} Department of Health Management & Informatics
\textsuperscript{3} 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.
Background

- MCR-ARC:
  - 2005 - Katrina
  - 2008 – Audit
- MoSTRA – 2010 Annual Meeting
  - Informal comments - Hospital registrars & other cancer reporters
  - Conclusion: Best practices not in place in many facilities
• Examples:
  • DC response contained MD’s credit card application
    • What did the credit card company receive?

• Records w/ PHI
  • Not double wrapped
  • Torn envelopes
Registrars should not rely on others to ensure the security of their data/records.

Creating awareness of potential issues should allow registrars to improve their registry’s security, and

Educate others in their own institution.

The goal –

- prevent unauthorized access to data; and
- eliminate processes that may result in a data breach.
What is the biggest threat to the government enterprise computing environment?

- Employees: 59%
- Privileged Administrators: 13%
- Hackers, cyber criminals: 15%
- Outsiders, including contractors: 9%
- Other: 5%

Wegand, S. Federal Computer Week, Volume 24 Number 20, p32.
Survey: e-mailed to 59 electronically reporting hospitals
- # cases varies from c. 100 - 1000s
- Several non-CoC
- Response rate - 40%

Possible bias:
- Hospitals with poor data security practices - less likely to respond?
- # of beds – not asked
- Anonymous – size, CoC
Survey - Security Measures

- Security measures - changing due to fewer paper documents
  - Respondents with entirely electronic records – 37%
  - All paper – 1 respondent
  - Combination – all others
Survey – Physical Security

- The majority of facilities have many basic data security practices in place
  - Secure fax machines/computers
  - Locked file cabinets in secure locations
  - Patient access restrictions to areas w/patient data
  - 60% said custodial services provided after work hours
Facility size not a good indicator of data security or practices

- A small facility may be small but have excellent security
- A large facility may not have all security measures in place
A few registrars do not know where to find institution’s data security policies & procedures

The majority have attended/participated in data security awareness/education program at hospital (class or online)
Two-thirds said registry job descriptions/evaluations included information about data security expectations.

99% said consequences for failure to abide by data security P&P have been communicated.
All but one hospital required the use of “strong” passwords.

Registrars who work remotely felt there were adequate security measures in place.
All registrars indicated paper materials were disposed of securely
- Joplin (more later)

However, 60% said follow-up letters are not sent in tear-proof envelopes

All said their electronic data was appropriately protected
- Joplin again (later)
c. ¼ of the registrars did not know if a risk analysis had been conducted or if their registry had been reviewed during a risk analysis.
Initial survey responses created additional questions
- Disaster plans (including off-site backup)?
- Computer OS (to see if encryption available)?
- Use of encrypted e-mail?
Education/ Awareness Program

- Newsletter supplement to include security checklist (best practices)
- Glossary of data security terminology
- Live Meeting presentation
- Info in each quarterly newsletter
Disasters & Data Security

- Lessons from Katrina & Rita
  

- Disaster Recovery – Lessons from Tulane’s Response to Katrina
  

- Rebuilding Healthcare in Post-Katrina New Orleans
  
The patient has a right to feel confident that all identifiable information about him/her possessed by the cancer registry will be kept confidential unless he/she waives the privilege, or release of the information is compelled by statute, regulations or other legal means.
Early Lessons from Joplin tornado

- EHR migration started in May 2011
  - incomplete
- All previous records are paper
  - still abstracting 2010 cases
- Offsite data backup/storage (multiple servers – in another city, in other destroyed buildings on hospital campus, etc.)
  - Not sure where cancer registry data stored/backed up.
Melamedia LLC – track HIPAA & Breach Enforcement for Free

http://www.melamedia.com/enforcement.php

Healthcare IT news – published in partnership with HIMSS

http://www.healthcareitnews.com

Government Computer News (GCN) -
http://gcn.com

Federal Computer Week -
http://FCW.com

Government Health IT -
http://www.govhealthit.com/
Questions?
ColeN@health.missouri.edu