Central Cancer Registry:

Documenting the Security of your Information Technology (IT) Infrastructure

Joseph D. Rogers

Team Lead

Cancer Surveillance Branch

Division of Cancer Prevention and Control

National Center for Chronic Disease Prevention and Health Promotion

June 22, 2011

Data Security – Why is it important?

- **Cancer registry data contains Personally Identifying Information (PII) that can be used for illicit purposes**
  - *Identity theft*
- **A person's medical history can be used to**
  - *obtain prescription medication fraudulently*
  - *embarrass or blackmail the person*
  - *increase insurance premiums*
- **Health care providers could use this breached data**

Data Owner Responsibility

- Protect Data
- Apply Software Patches
- Implement Multiple Levels of Security
- Audit and Penetration Tests
- Monitor Database Activity
- Implement Database Intrusion Detection
- Encryption:
  - *Data At Rest (DAR)*
  - *Data in Motion (DIM)*
  - *Data In Use (DIU)*

Planning for Data Security

- Who has access to the databases?
- How are administrative passwords stored?
- What are the policies for auditing system security and looking for suspicious activity?
- What is the procedure if security is breached?

Developing a Security Policy

- Designate a Chief Technology Officer (CTO)
- Find out if you have a security policy
- Develop a security policy
- Execute the policy
- Review and update the policy

Risk Assessment and Management (Part 1)

- **Security Document with Standards from—**
  - *The National Institute of Standards and Technology (NIST)*
  - *Federal Information Processing Standard 140 (FIPS)*
  - *The North American Association for Central Cancer Registries (NAACCR) Standards for Cancer Registries Volume III, chapter 6, "Security and Confidentiality"*
  - *Certification and Accreditation Process Guide, as referenced in the CDC Unified Process*

The Security Document

- Risk assessment and management
- Networking and privacy security policies
- Encryption of data on mobile services and portable media
- Plans for encryption of data in databases
- Disaster recovery plans
- Ongoing security training
- Audit security policies regularly
- Review and update the security document

What does CDC Provide?

- **Certification and Accreditation (C&A) on all systems deployed within CDC**
- **All registry products created by CDC have passed the CDC C&A processes**
- **Checklists details how CDC or the administrator addresses the National Institute of Standards and Technology (NIST) requirements**
  - *This model might be used to assist in meeting the data sharing requirements in Memorandum of Understanding (MOU)'s and Authorization to Operate (AtO)'s*
  - *Provides a general understanding of data security and how to address Memorandum of Understanding (MOU)'s and Authorization to Operate (AtO)'s to obtain cancer registry data sharing agreements*

What is the CDC Certification and Accreditation (C&A) Process

- Security certification is a comprehensive evaluation of CDC's management, operational, and technical security controls for an information system
- Security accreditation is CDC management's official decision to authorize an information system to operate

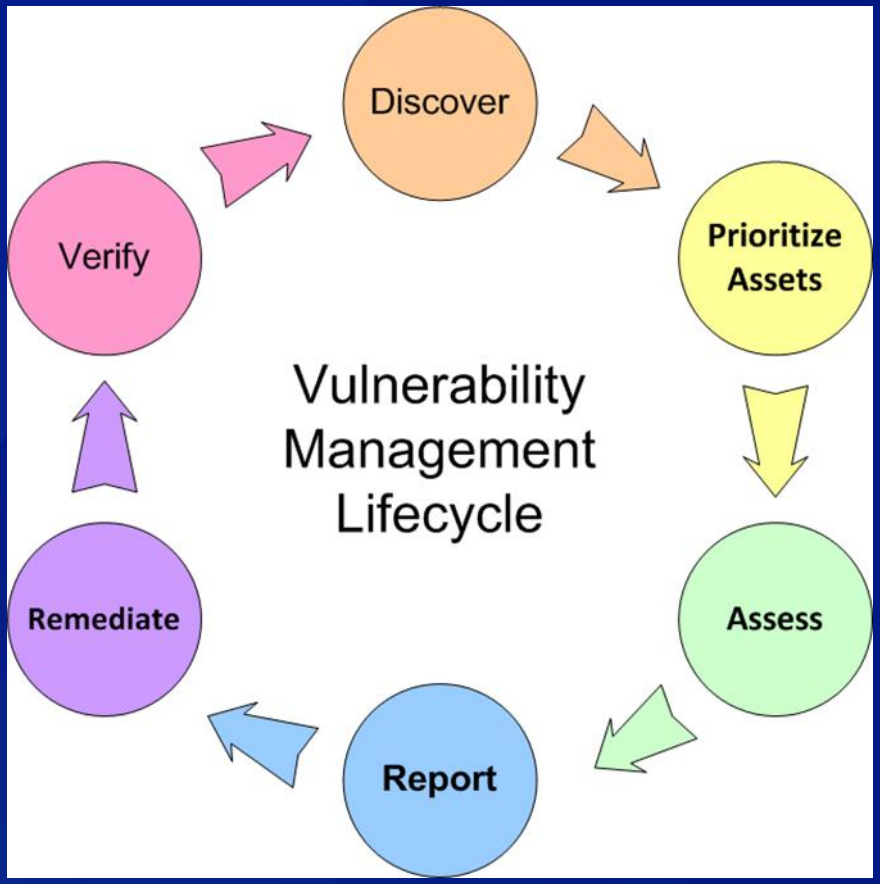
What is a Data-Sharing Agreement?

- Obtaining data sharing agreements
- Data sharing agreements provide a level of assurance
- Documentation that the requesting organization has addressed National Institute of Standards and Technology (NIST)-required minimum security
- Memorandums Of Understanding (MOU) and Authority to Operate (AtO) agreements

Internal Audit

- Achievement of the parent organization's objectives
- Appropriate assessment of risk
- Reliable internal and external reporting
- Compliance with applicable laws and regulations
- Compliance with NPCR's standards for the registry

Vulnerability Management Life Cycle - Diagram



Federal Information Processing Standards (FIPS) Security Levels

- **FIPS 140-2 defines four levels of security—**
  - *FIPS 140-2 Level 1:*
    - *lowest level*
  - *FIPS 140-2 Level 2:*
    - *requirement for tamper-evidence*
  - *FIPS 140-2 Level 3:*
    - *physical security mechanisms*
  - *FIPS 140-2 Level 4:*
    - *highest level of security*

Conclusion

- **How to address and document the security of the Information Technology (IT) Infrastructure**
- **Sources provide successful methods**
- **Data Security should not be "only" used to address the outside organizations directives**
  - *Protect image of Central Cancer Registry's (CCR)*
  - *Future funding*

Acknowledgements

- Scott Van Heest, CDC/NPCR: SVanHeest@cdc.gov
- Sanjeev Baral, Northrop Grumman Contractor for CDC/NPCR: SBaral@cdc.gov

Thank You!

Joseph D. Rogers, CDC/NPCR
Team Lead
770-488-4701
JRogers@cdc.gov

For more information please contact Centers for Disease Control and Prevention

1600 Clifton Road NE, Atlanta, GA 30333
Telephone, 1-800-CDC-INFO (232-4636)/TTY: 1-888-232-6348
E-mail: cdcinfo@cdc.gov Web: www.cdc.gov