Texas Cancer Registry

TEXAS Department of State Health Services

Data Security

John Hopkins
Core Operations Manager

Melanie Williams, Ph.D.
Branch Manager

Texas Cancer Registry
April 17, 2009

Background

- TCR receives approximately 200,000 reports from over 500 reporters annually
- High volume of data
- Located in large state agency
- Needed to formalize process more fully due to increasing oversight, more stringent requirements, and inconsistency of practices within the TCR
- Tremendous variation of reporter understanding, resources, and capability to safe guard data

Purpose

- Customers and stakeholders trust the TCR will protect confidential information
- This policy and procedure is part of an overall risk management strategy
- Covers administrative, physical and technical safeguards of confidential information
- The TCR has a responsibility to prevent breaches of confidential information and respond decisively if a breach does occur
- Covers procedures and actions in the event of a breach of confidential information

TCR Data Security Philosophy

- Must meet all state, federal requirements, including those of the VA
- Rigid in requirements but attainable
- Can not be complacent about data security-related education or communication
- Policy must be comprehensive, covering both technological and human components
- Never under-estimate the human component
  - e.g., our ability to interpret policy differently, find a new scenario that is not addressed, is not as clear as it could be, or staff ability to not follow…

Improvement Process

- Reviewed state and federal data security requirements
- Reviewed agency and state IT requirements and policies
- Reviewed other state cancer registry requirements and policies
- Sought and consulted with Agency data security subject matter experts
- Reviewed current business needs and practices

Elements of the TCR Policy

- Background and Overview
- Responsibility and Authority
- Related Policies
- Definitions
- Applicability
- Confidentiality and Non-Disclosure Agreement

Elements of the TCR Policy

- Training
- Risk Assessment
- Physical Safeguards
- Items specific to NPCR, VA, and own Agency Requirements
- Exchange of Confidential Data
- Acceptable Encryption Methods

Elements of the TCR Policy

- Internet and Intranet Security
- Termination of Access
- Security Incident Procedures
- Forms
  - TCR Confidentiality and Non-Disclosure Agreement
  - TCR Breach of Confidentiality Report

Elements of the DSHS-IT Policy

- Administrative Security Controls
  - Information security policy
  - Computer usage policy/handbook
  - Information Security Standards and Guidelines
  - Annual training and certification for Security and Computer Usage
  - Signed Computer Usage Agreement
  - Computer Incident Response Plan
  - Information Security Team

Elements of the DSHS-IT Policy

- Physical Security Controls
  - Workplace has on site security (guards)
  - Locked and security card access doors
    - Verified who had keys and access
  - Smoke, fire detection with current test
  - Fire suppression available and current test
  - Uninterruptible power source available

Elements of the DSHS-IT Policy

- Notable Technical Security Controls
  - Annual vulnerability scanning performed on system
  - IT security audit performed every 2 years
    - Identified need for encryption on lap tops
    - Identified access scripts into central registry database system were imbedded with passwords
    - All corrected

Elements of the DSHS-IT Policy

- Notable Technical Security Controls
  - Current Anti-virus
  - System patches/fixes applied within 2 weeks of release/notification
  - Authentication by use of unique user IDs, and strong, effective passwords
  - Authorizations, permissions, rights, and privileges
  - System and data backups are performed daily

Responsibility and Authority

- Eight (8) laws cover the TCR's responsibility regarding confidential information
- Twelve (12) policies relate to the TCR's procedures regarding confidential information
- The CESB Manager is ultimately responsible for ensuring compliance, but
- Everyone with access to confidential information bears a level of responsibility
  - Read, understand and follow the policy and procedure
  - Receives annual training
  - Frequent reminders and availability for clarification

Important Definitions

Breach of Confidential Information

an incident in which confidential information is known to have been:

1) accidentally or intentionally released verbally, electronically, or by paper media, to an entity or person that by law does not have a right or need to know, **or**

2) purposefully accessed either in person or electronically by an entity or person that by law does not have a right or need to know

Important Definitions

Confidential Information

a) demographic and/or cancer diagnosis and treatment information that would or could result in the identification of the individual, treating physician or reporting institution should that information be released

b) information that is excepted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal law

Important Definitions

Confidential Information

c) any information by which the identity of a client or employee can be determined either directly or by reference to other available information if the identity cannot be disclosed under federal or state law

Applicability

- Applies to:
  - TCR Employees
  - Temporary Employees
  - Contractors
  - Volunteers
  - Researchers
  - Anyone who is granted access to confidential data

Confidentiality and Non-Disclosure Agreement

- New hires, temporary employees, contractors, volunteers and anyone else allowed access to confidential information must complete form
- Remains in effect after employment or end of business/educational relationship

Training

- Overview of this policy and procedure required for all persons who will access confidential information

- TCR employees and contractors must also complete annual DSHS Computer Usage and Information Security Training

IT Risk Management

- To assess risk to systems and confidential information
- Audits conducted on a biennial basis
- Includes:
  - Threat Assessment
  - Security Risk Analysis
  - Mitigation Plan (if needed)

Risk Management

- On a periodic basis, managers, supervisors and staff members conduct reviews and activities to ensure policies and procedures are understood, being followed and are updated as necessary (P.6)
- Information Technology reviewed as well by TCR staff, not just IT

VA Requirements

- Currently have all 7 VA Hospitals with signed agreements
  - Relationships with staff was critical
  - Made necessary changes based on their requirements
  - Continue to consider business processes and other questions related to possible procedural changes (i.e., consolidation)

VA Requirements

- Changes Included:
  - Limiting internal VA data access
    - Regional staff no longer process VA data
  - At-rest data encryption on server that meets Federal Information Processing Standard 140-2 (i.e., PGP NetFile Software)
  - Data are not placed on portable media
  - Updated data release policies, research, out-of-state data exchange

Physical Safeguards

- No exceptions
- Computer screens out of view of visitors
- Confidential information on any media or hard copy locked up at end of day
- No confidential information on hard drives

Physical Safeguards

- Transporting confidential information:
  - Hard copy documents in secure container and not visible in vehicle
  - Electronic files encrypted/password protected
  - Never left unattended in place or area to which unauthorized persons may reasonably gain access
  - When possible taken directly to the TCR office the same day
  - Never take to a private residence, place of business or outside of vehicle, EXCEPT:
  - May be moved from vehicle to overnight lodging or employee's residence when return to TCR office is impractical, but may not be left unattended in either of those locations

Physical Safeguards

- Access to TCR Offices
  - Visitors must sign in
  - Visitors escorted and accompanied by staff
  - Security systems must meet regulations and codes
  - Access to controlled areas must be limited
  - We do not loan out access cards or keys
  - Report lost or stolen access cards or keys
  - Server rooms must be locked at all times

Physical Safeguards

- Other Considerations
  - Shred hard copy documents or place in confidential shred containers
  - Password protect computers and laptops
  - Encrypt and password protect data on removable media
  - Use of removable media must be in accordance with DSHS policy
  - Before disposal of diskettes, CDs or removable media with confidential information sanitize according to standards

Exchange of Confidential Data

- Transmittal of confidential information in hard copy form by mail, overnight delivery service, or courier services is prohibited

- Secure FTP whenever possible

- Confidential information may only be sent on CD/DVD by overnight delivery service (not USPS)
  - Must be encrypted/password protected
  - Use interior envelope that is sealed/marked “confidential”
  - Passwords must be sent separately (mail, email or by phone)

Exchange of Confidential Data

- Fax transmissions permissible following safe practices
  - Fax in secure area
  - Fax number is verified prior to sending, programmed, and notice provided to recipient prior to faxing
- Training and demonstration materials and files must use fictitious or redacted information

Acceptable Encryption Methods

- All outgoing data (electronic or physical) must be encrypted/password protected
- Passwords must be provided separately
- WinZip Version 9 or later is preferred encryption software
- Removable media must allow data encryption and password protection

Internet & Intranet Security

- The use of email and/or email attachments, including encrypted email and/or attachments for the purpose of transmitting confidential information is prohibited

- Use secure servers when uploading or downloading confidential information

Termination of Access

- Upon separation of employee, contractor or other persons with access rights to computer systems, supervisor terminates access to:
  - Network (DSHS)
  - Email (DSHS)
  - Internet (DSHS)
  - SandCrab Applications (TCR)

Security Incident Procedures

- Notify supervisor or Team Lead immediately upon discovery
- Supervisor or Team Lead initiates immediate response to secure information and work area
- Notify Central Office and follow up with electronic copy of Report form

Security Incident Procedures

- CESB Manager must notify DSHS CIRT
  - TCR Process does not replace the CIRT process
  - All TCR staff must cooperate in CIRT process
- TCR Security Team established
- TCR Security Team examines reported or suspected breach and completes Report form
- Media contacts referred to TCR manager

Moving Forward

- The TCR Confidential Information Security Policy is not static
- Suggestions for changes, updates or improvements always welcome
  - Clarifications or omissions
  - Incorporate new requirements
  - Incorporate new technology
  - Incorporate new programs/processes
  - DSHS/HHSC policy/procedure changes
  - Implement Mitigation Plans (Risk Management)

Questions

Gracias