
Strategies for Protecting Sensitive Data

Susan Wyatt Sedwick, Ph.D., CRA
Associate Vice President for Research and
Director, Office of Sponsored Projects
The University of Texas at Austin



CIPSEA

- Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)
 - Provides strong confidentiality protections for statistical information collections sponsored by or conducted by more than 70 Federal agencies
 - Establishes uniform policy across Federal agencies
 - Authorizes data sharing among specified agencies (Bureaus of Economic Analysis, Labor Statistics and Census) to include identifiable data
 - CIPSEA data may only be used for statistical purposes
-

Penalties for Non-Compliance

- Class E felony with imprisonment of not more than five (5) years and/or
- Fine of not more than \$250,000

CIPSEA Implementation Guidance

- Implementation Guidance issued June 15, 2007 [FR V. 72, No. 115 Pg. 33362]
- Harmonizes principles and processes and sets minimum standards for safeguarding confidential statistical information
- Utilized best practices for handling confidential statistical information
- Addressed intersection between CIPSEA and Privacy Act of 1974 for non-statistical uses

What does CIPSEA protect?

- Defined *personally identifiable information*
 - Information that can be used to distinguish or track an individual's identity such as name, SSN, or biometric information
- Provided example of *indirect identification*
 - Using information in conjunction with other data elements to reasonably infer the identity of a respondent such as a combination of gender, race, date of birth, geographic indicators, or other descriptors

Authority

- Federal agencies empowered to make determination about the sensitivity of their information used for *statistical purposes* under a pledge of *confidentiality*
- Applies to local and State governments collecting data for Federal agencies
- Restrictions on use of CIPSEA
- Special procedures required for use of laptop computers, PDAs, zip drives, floppy disks, CD-ROMs or any other IT devices

Minimum Requirements

- Inform respondents about the confidentiality protection and use of the information
- Minimize risk of disclosure including training of employees with access
- Restricts use to statistical purposes
- Protect against inference of identities through direct or indirect means
- Supervise and control agencies who have access to such data

Minimum Standards

- All persons with access understand his/her responsibility related to maintaining confidentiality of information
- Monitoring procedures for collection and release
- Evaluating the reason for and controlling access
- Maintaining physical and information systems security

Required Training

- Overview of protection procedures
- Limit access to those with a “need to know”
- Physical and information systems security procedures must be in place
- Penalties

Inspections of Federal Agencies

- Assess and document that written procedures and security plan are adequate
- Data can be released prior to inspection but written procedures required
- Inspections must be performed and prior notice of inspection not required

Examples

- Bureau of Labor Statistics
- National Institute of Child Health and Human Development
- Institute of Education Statistics
- Toledo Adolescent Relationships Sensitive (TARS) Data
- Texas Higher Education Coordinating Board (THECB)

Minimum Procedures

- Confidentiality is protected
- Confidential information is used exclusively for statistical purposes
- Access is controlled and only authorized persons have access
- Persons having access understand obligations including penalties
- Roles and responsibilities for contact persons
- Procedures for return or destruction of confidential information
- Termination provisions
- Provisions for inspection

Agreement Terms

- List of person(s) with access
- Certification that all persons with access have completed confidentiality training
- Signed non-disclosure forms for all persons with access
- May require background information
- Penalties that may be imposed by agency
 - Civil and Criminal

Sensitive Data Control Plan

- Commitment
- Specific requirements and need for and use of sensitive data
- Physical security
- Information security
- Personnel screening
- Training and awareness
- Compliance assessment
- Termination
- Certification forms

Protection of Sensitive Digital Data

- UT Austin Policy
 - <http://www.utexas.edu/its/policies/researchers/index.php>
 - Required Practices
 - Data Classification Standard - Category I Data
 - Anti-virus, anti-spyware and firewall software provided at no cost
 - Requires use of application-level security
 - Minimum security standards for systems
 - Physical security
 - Assistance with destruction
-

Digital Information Security

- Commercially available encryption
 - *Safeboot*
 - Password protection screen savers
 - Secure when not in use
-

Approach

- Centralized security
- Student support
- “Unit” data security plans

Questions

Susan Sedwick
sedwick@austin.utexas.edu

