

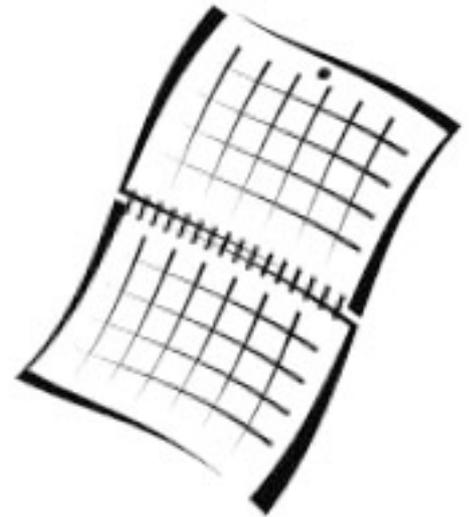
NAHMS Confidentiality Training



You need this training if you...

- Participate/ collaborate in a NAHMS CIPSEA study
- Need access to NAHMS data protected by CIPSEA
- Manage the information systems that store NAHMS CIPSEA data
- Need access to the NAHMS data lab

This is an annual requirement



Why do I need to know?

Protecting identifiable and confidential data is:

- Critical to mission success
- The law!
- The right thing to do



Why do I need to know?

It's in the news!



There are serious public concerns with issues of privacy and confidentiality

Critical to Mission Success

Protecting respondents' identifiable and confidential information builds trust and confidence



Critical to Mission Success

Improper handling or misuse of survey data could jeopardize NAHMS' ability to collect, analyze, and disseminate information



Critical to Mission Success

- Any improper disclosure or use of confidential information will:
- Undermine NAHMS' credibility and public trust
- Impair NAHMS' ability to obtain similar information in the future
- Negatively affect the accuracy of the information reported by respondents



It's the Law

Identifiable and confidential information is protected by federal law



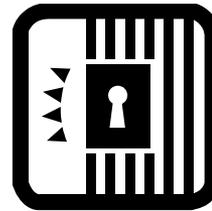
- Privacy Act
- 2008 Farm Bill, section 1619
- Confidential Information Protection and Statistical Efficiency Act (CIPSEA)

It's the Law

Serious penalties can be assessed for intentional disclosure



\$250,000 fine



5 years imprisonment

These penalties are specific to CIPSEA-protected data



Or BOTH!

3 Things You Need to Know About CIPSEA

- CIPSEA provides the highest level of data protection
- CIPSEA requires that:
 - A pledge of confidentiality is made to the respondent
 - The data are used **ONLY** for statistical purposes
- There are serious personal penalties for the intentional disclosure of CIPSEA-protected data

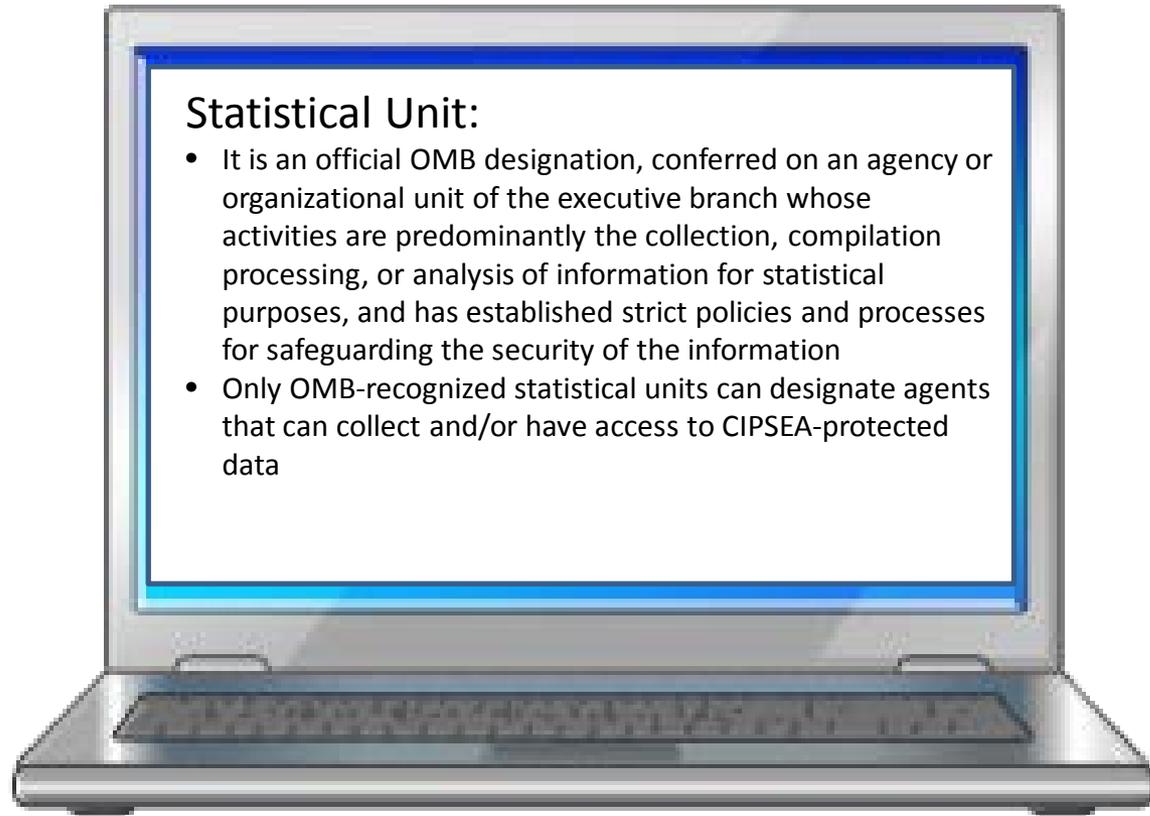


CIPSEA-protected data are exempt from FOIA requests, judicial subpoenas, and presidential orders.



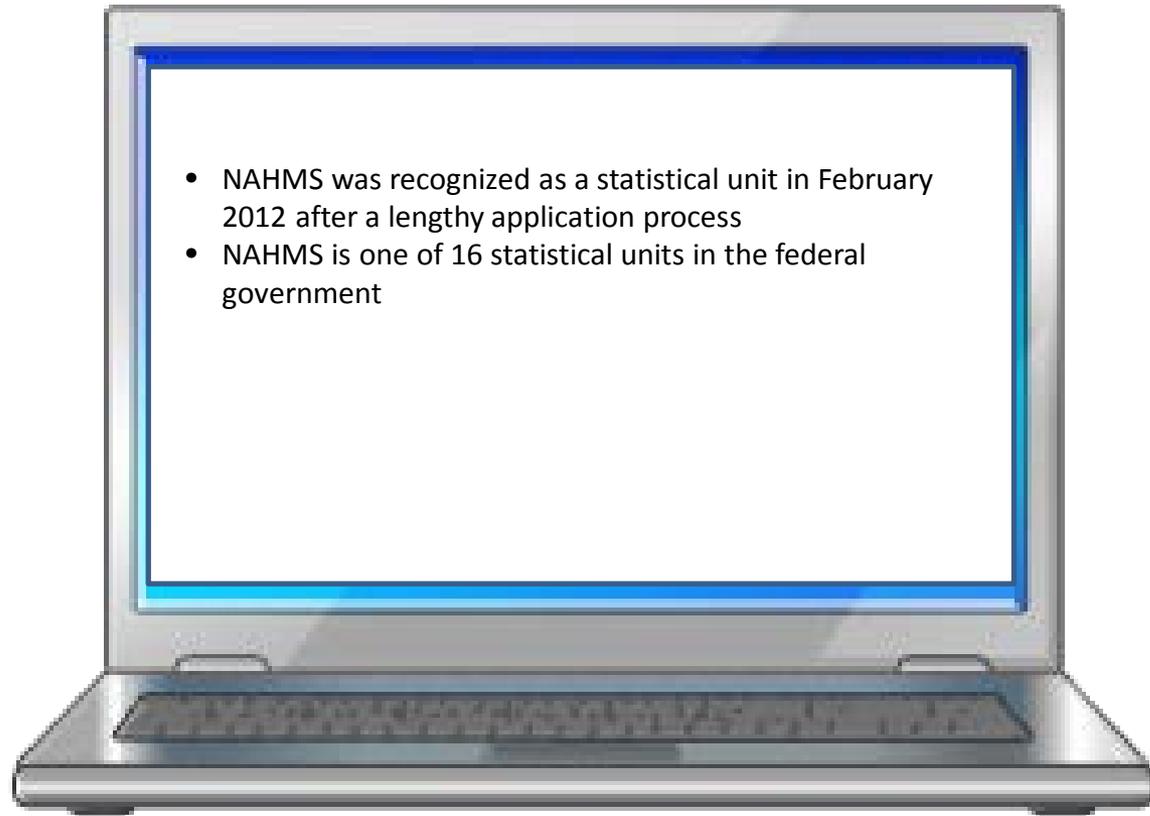
Definitions

- Statistical Agency/ Unit
- Identifiable and Confidential Information
- Pledge of Confidentiality
- Statistical Purposes
- Disclosure
- Agents

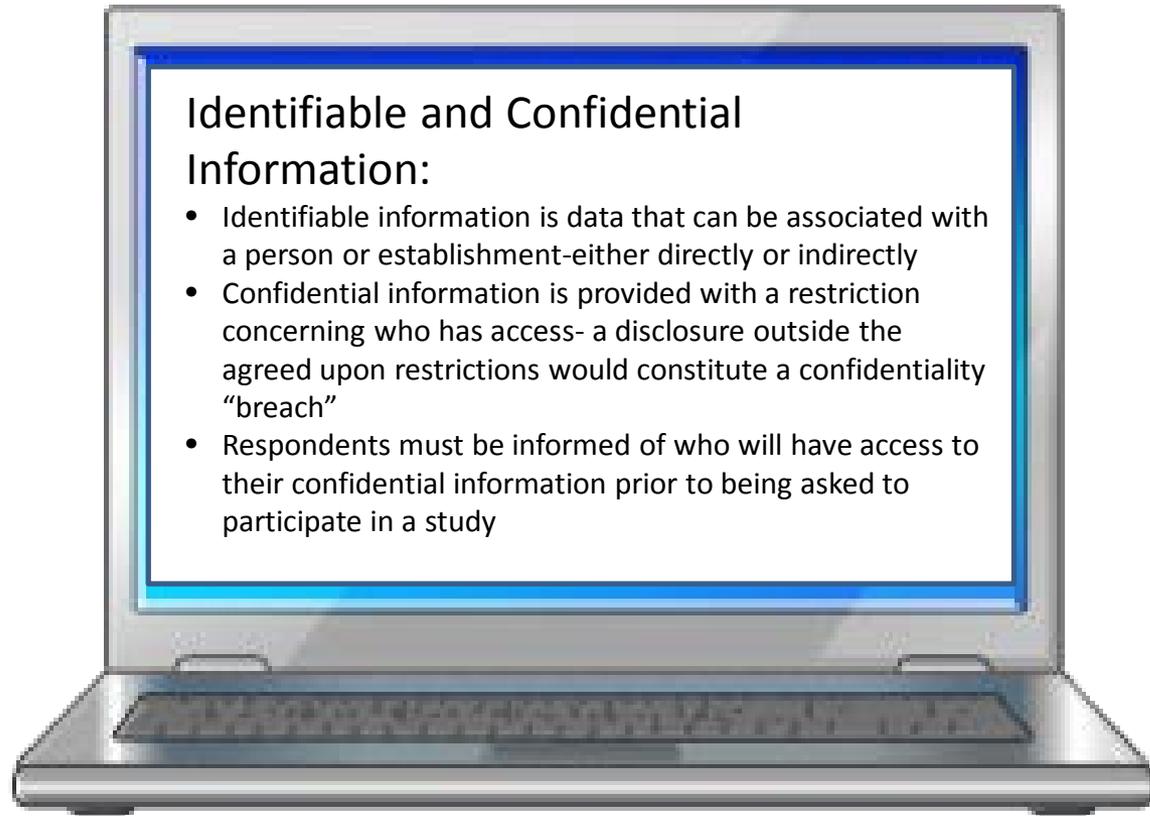


Statistical Unit:

- It is an official OMB designation, conferred on an agency or organizational unit of the executive branch whose activities are predominantly the collection, compilation processing, or analysis of information for statistical purposes, and has established strict policies and processes for safeguarding the security of the information
- Only OMB-recognized statistical units can designate agents that can collect and/or have access to CIPSEA-protected data

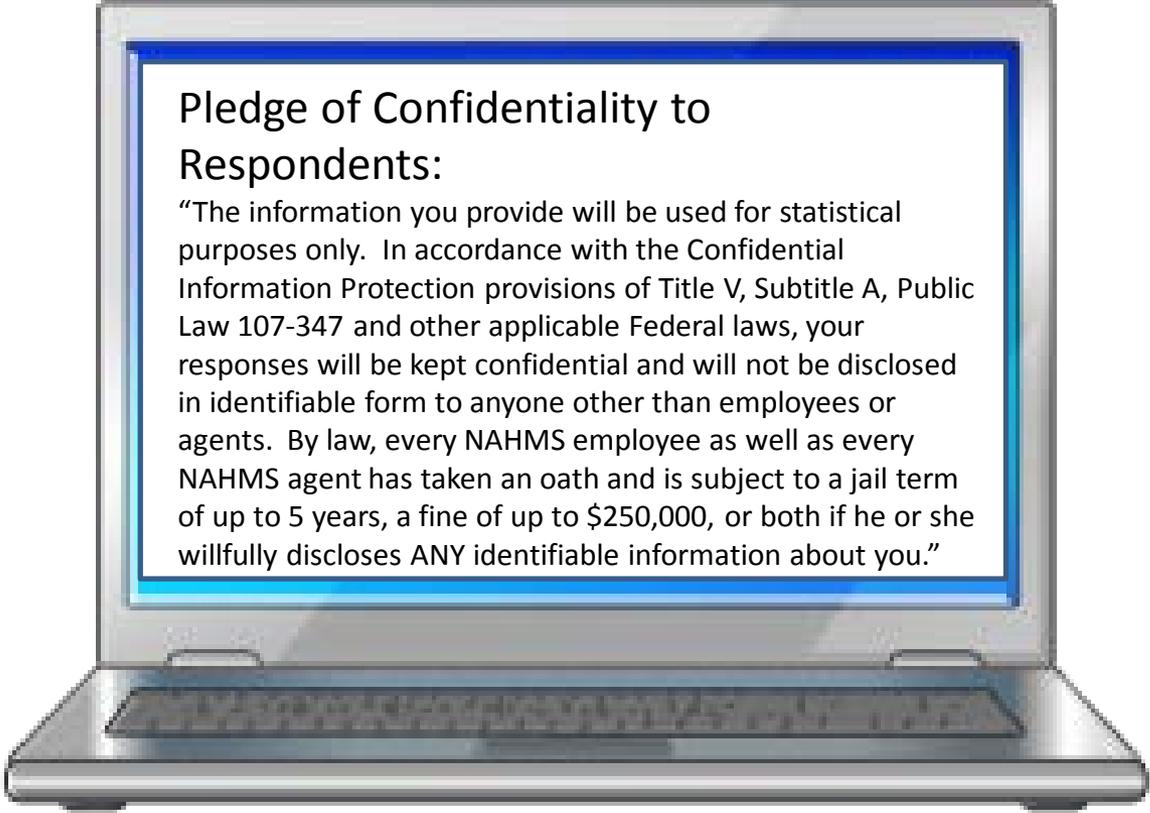


- NAHMS was recognized as a statistical unit in February 2012 after a lengthy application process
- NAHMS is one of 16 statistical units in the federal government



Identifiable and Confidential Information:

- Identifiable information is data that can be associated with a person or establishment-either directly or indirectly
- Confidential information is provided with a restriction concerning who has access- a disclosure outside the agreed upon restrictions would constitute a confidentiality "breach"
- Respondents must be informed of who will have access to their confidential information prior to being asked to participate in a study

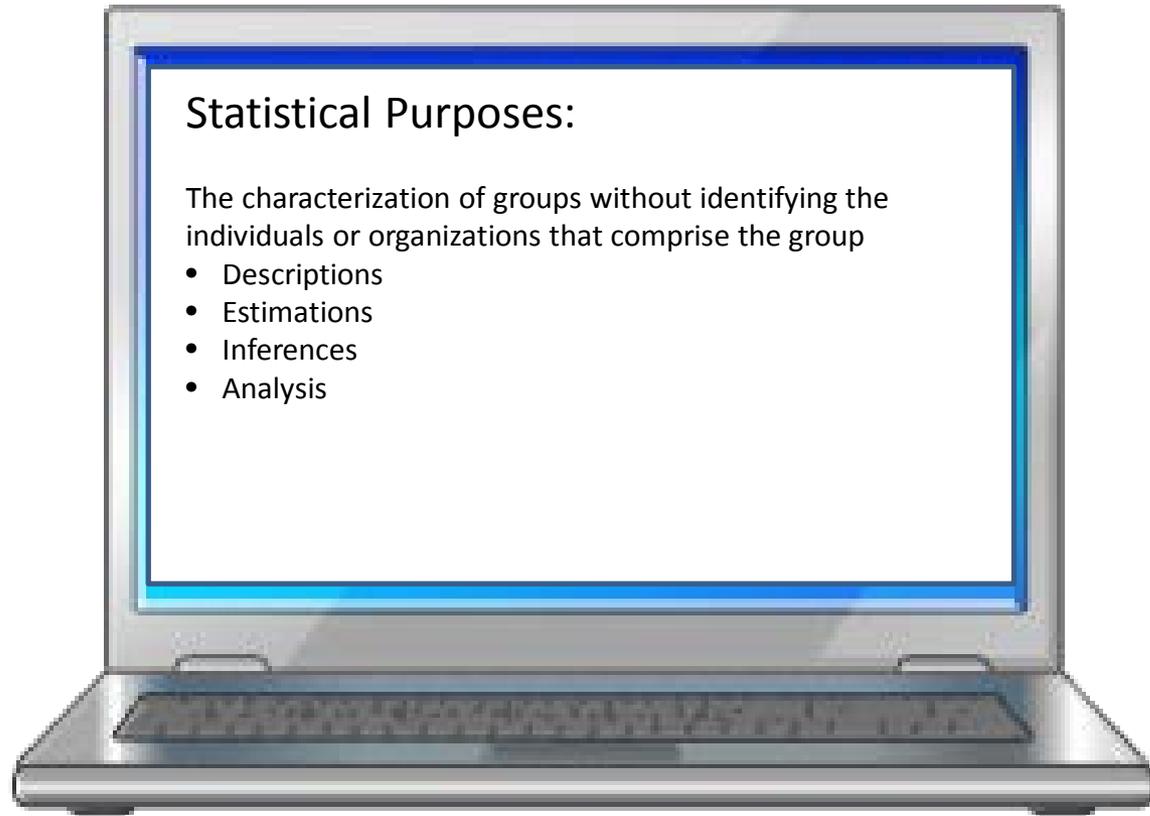
A silver laptop computer is shown from a front-facing perspective. The screen is open and displays a white rectangular area with a blue border. Inside this area, the text of a confidentiality pledge is written in black. The laptop's keyboard and trackpad are visible below the screen.

Pledge of Confidentiality to Respondents:

“The information you provide will be used for statistical purposes only. In accordance with the Confidential Information Protection provisions of Title V, Subtitle A, Public Law 107-347 and other applicable Federal laws, your responses will be kept confidential and will not be disclosed in identifiable form to anyone other than employees or agents. By law, every NAHMS employee as well as every NAHMS agent has taken an oath and is subject to a jail term of up to 5 years, a fine of up to \$250,000, or both if he or she willfully discloses ANY identifiable information about you.”



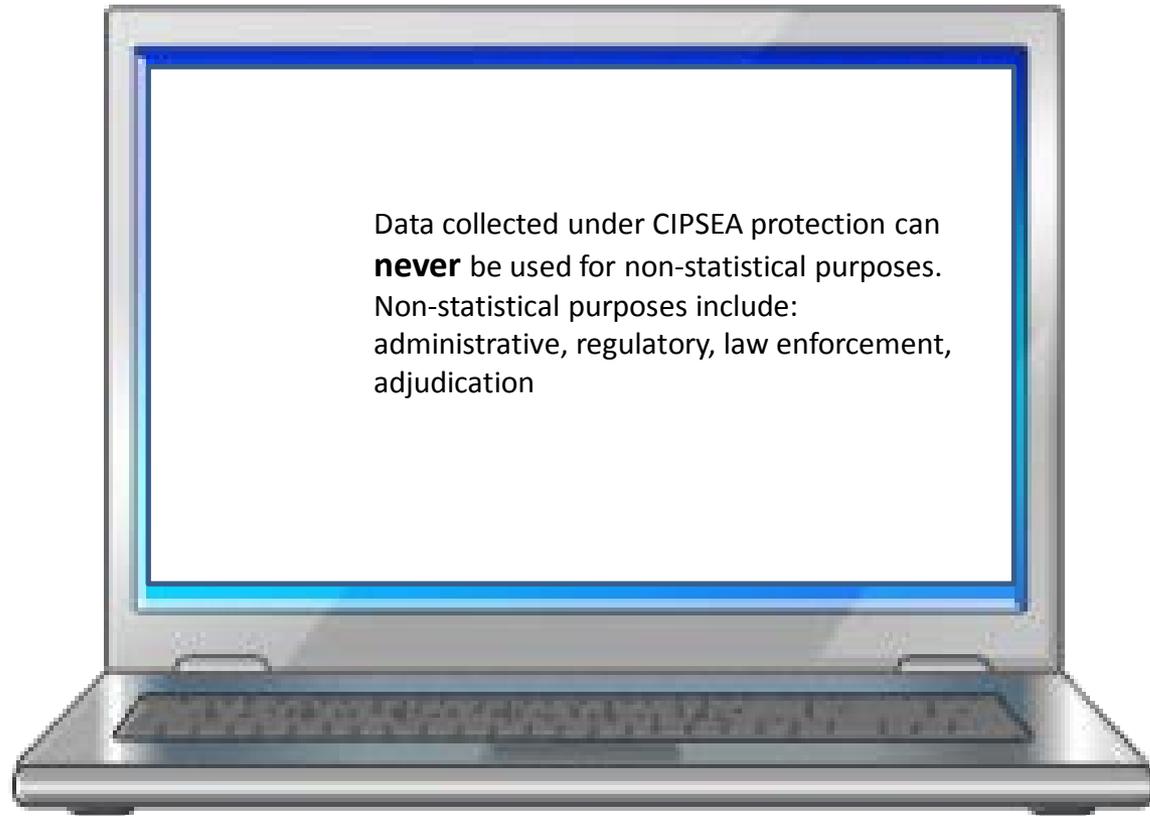
Promises made are promises kept



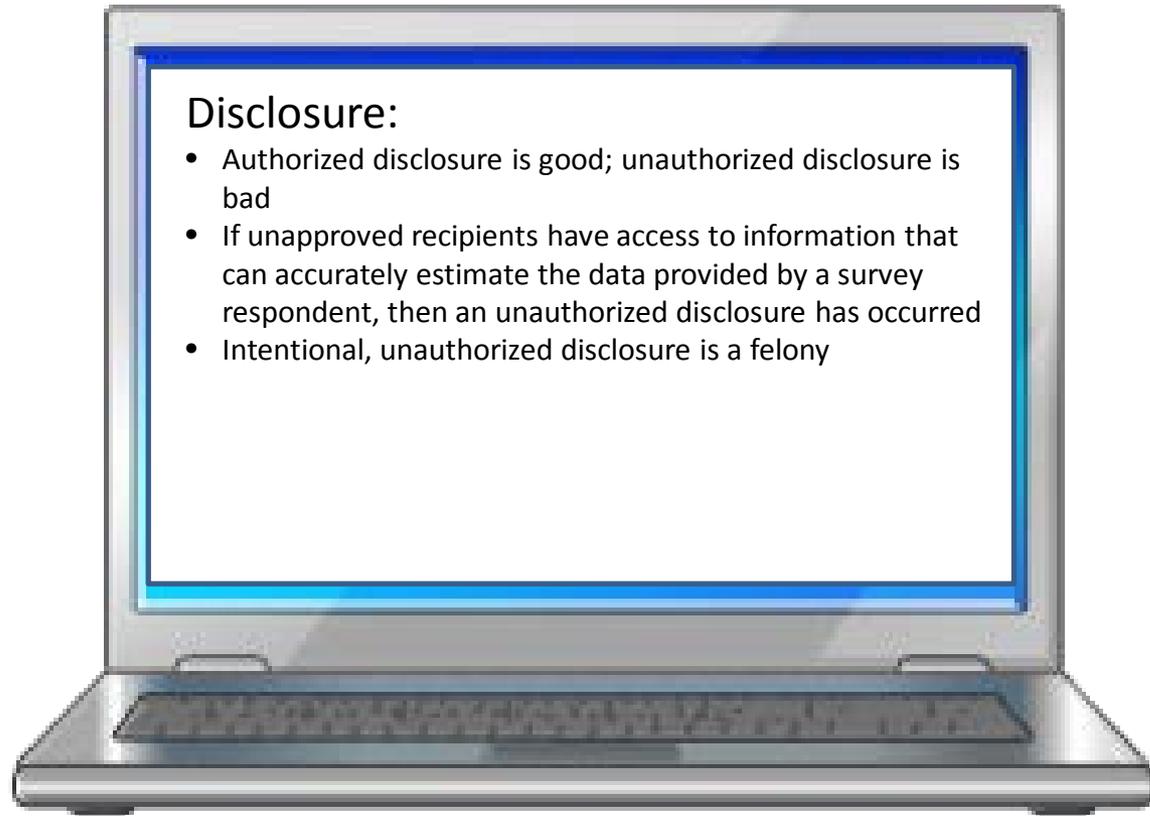
Statistical Purposes:

The characterization of groups without identifying the individuals or organizations that comprise the group

- Descriptions
- Estimations
- Inferences
- Analysis

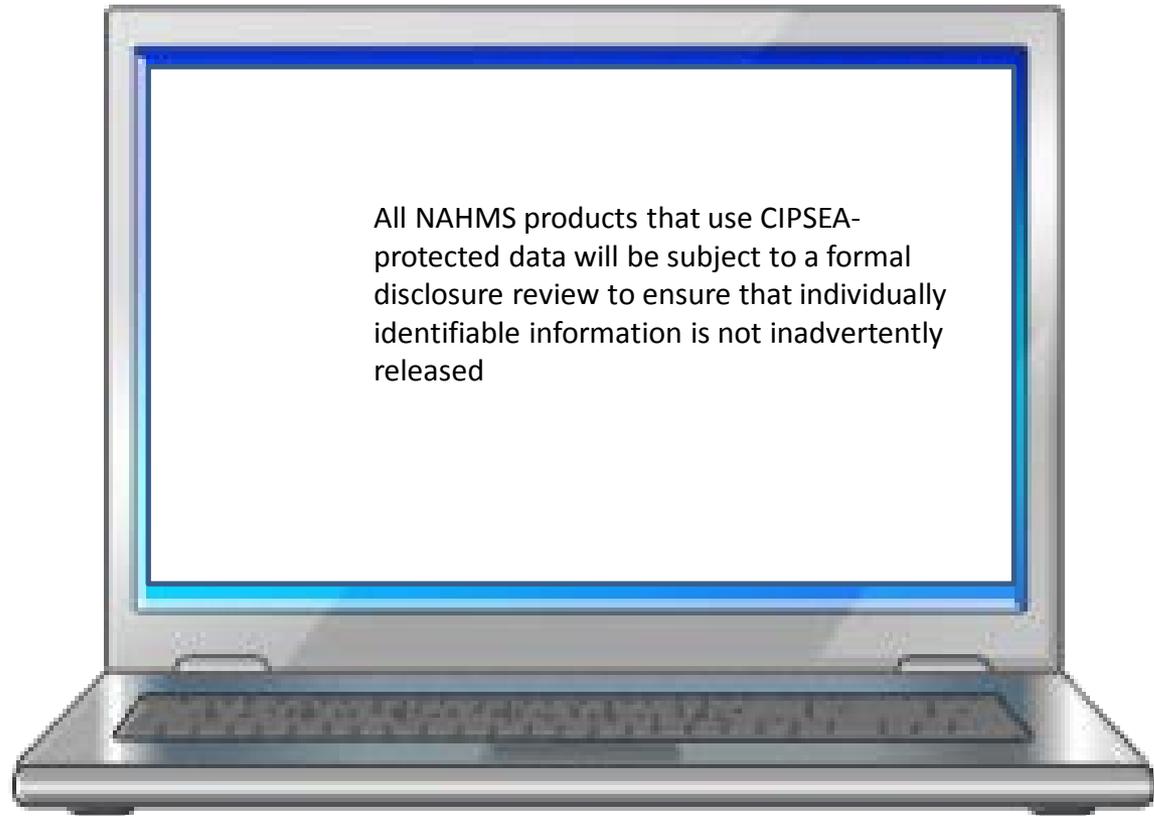


Data collected under CIPSEA protection can **never** be used for non-statistical purposes. Non-statistical purposes include: administrative, regulatory, law enforcement, adjudication



Disclosure:

- Authorized disclosure is good; unauthorized disclosure is bad
- If unapproved recipients have access to information that can accurately estimate the data provided by a survey respondent, then an unauthorized disclosure has occurred
- Intentional, unauthorized disclosure is a felony

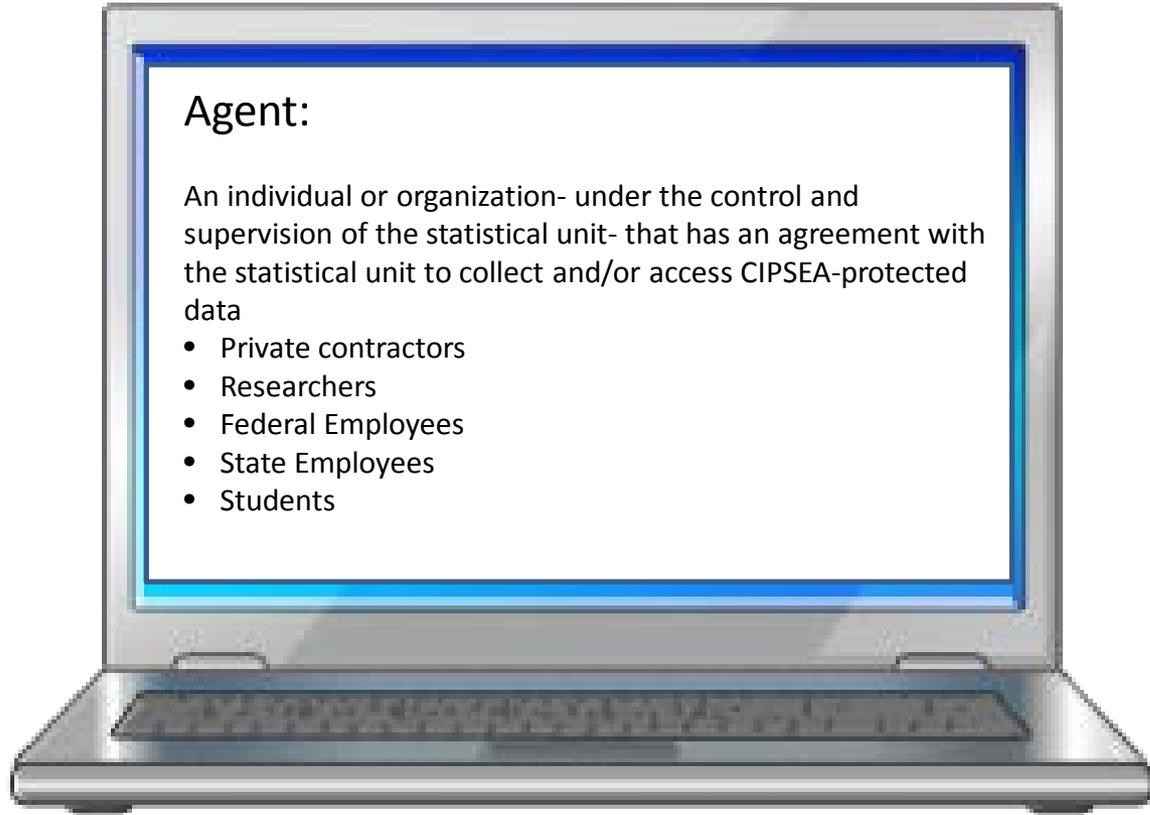


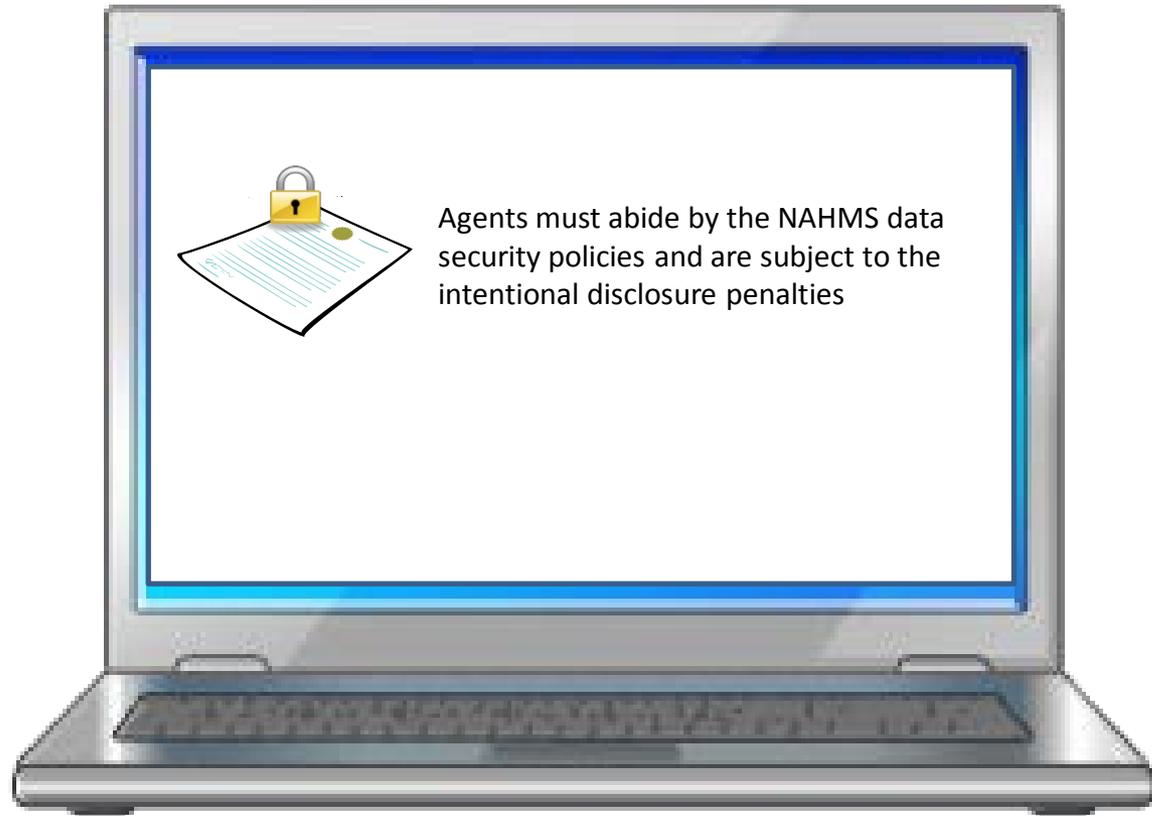
All NAHMS products that use CIPSEA-protected data will be subject to a formal disclosure review to ensure that individually identifiable information is not inadvertently released

Agent:

An individual or organization- under the control and supervision of the statistical unit- that has an agreement with the statistical unit to collect and/or access CIPSEA-protected data

- Private contractors
- Researchers
- Federal Employees
- State Employees
- Students

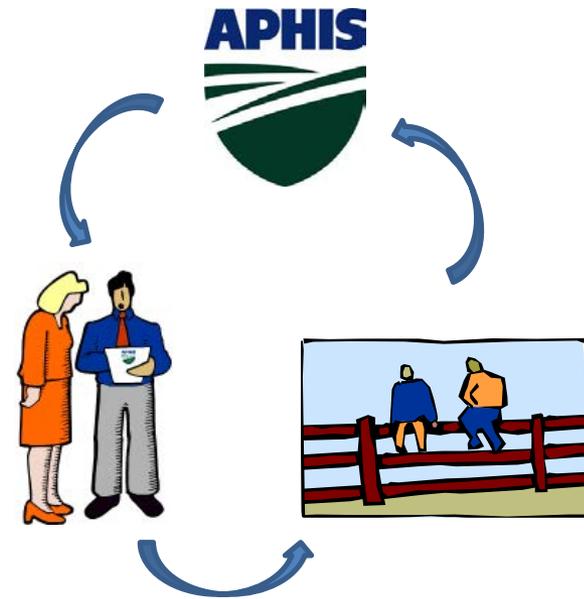




Agents must abide by the NAHMS data security policies and are subject to the intentional disclosure penalties

NAHMS Study Cycle

- NAHMS Employees
- Study Coordinators
- Data Collection Agents



NAHMS Employees

- Develop respondent sampling lists containing PII
- Distribute lists to field coordinators
- Receive completed questionnaires
- Analyze data
- Produce reports



NAHMS Employees- Role in Protecting Information

- Keep completed surveys in the NAHMS data lab
- Ensure validated electronic SAS datasets are stored on the secure NAHMS SharePoint site
- Perform a disclosure review before releasing final reports to the public
- Handle CIPSEA-protected data in a manner that prevents unauthorized disclosure



Study Coordinators

- Ensure data collectors complete training and disclosure forms
- Receive respondent lists
- Distribute lists to data collectors

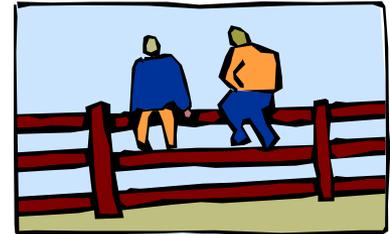
Study Coordinators- Role in Protecting Information

- Ensure data collectors have completed training and nondisclosure agreements in place prior to sharing producer sampling lists
- Distribute producer sampling lists in a manner that maintains producer confidentiality
- Collect and destroy producer sampling lists after all interviews have been completed



Data Collectors

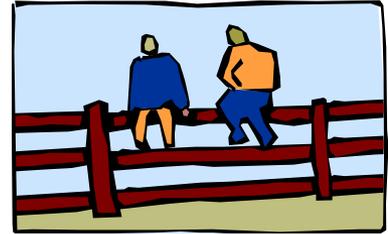
- Also known as “NAHMS Agents”
- Complete training
- Receive respondent lists
- Interview producers
- Securely return completed questionnaires



Data Collectors-

Role in Protecting Information

- Keep personally-identifiable information secured at all times in the field
- Shred cover sheets and sampling lists
- Follow directions for returning questionnaires to NAHMS



CIPSEA is implemented with

- Policies
- Administrative Processes
- Physical Security of Data
- Information System Security



CIPSEA sets minimal standards for safeguarding confidential information. A statistical unit is required to establish policies and processes that safeguard, to the extent possible, CIPSEA-protected data.

Policies

- Monitoring Data Collection
- Considering Requests for Information
- Granting Access to Confidential Data
- Specifying Individual Responsibility for Protection of Data



Agencies must ensure that each person having access to identifiable information understands his/her responsibility related to maintaining the confidentiality of that information, and signs a non-disclosure statement.

Administrative Processes

- Contracts and agreements
 - MOU or Cooperative Agreement
 - Non-Disclosure Agreement
- Confidentiality Training
- Disclosure Review Board
- Record Keeping
 - Repository of Assurances
 - Privileges Granted
- Reports
 - Annual CIPSEA Report



Formal agreements are required for

- Agents
- Researchers
- Respondents
- Project team members

Physical Security of Data

- Controlled-Access Data Lab
- Password-Protected Computers
- Sensitive Information Locked in Vehicles, Cabinets, or File Drawers
- Encrypted Data



Data must be protected, to the extent possible, from unauthorized access.

Information System Security

- Technical Safeguards that Assure
 - Data Security,
 - Data Integrity, and
 - Data Availability
- Threats and Hazards Mitigation
- Private Domain on a Secure Government Network used for Data Storage



Access to data is strictly controlled. Data are protected against intentional and accidental corruption. Data are accessible to authorized individuals when needed.

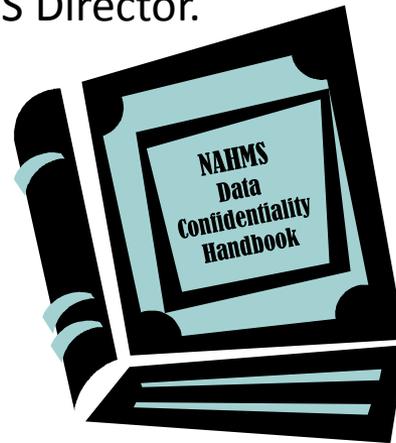
Your Responsibilities



DO

- **Read** the NAHMS manual on confidentiality
- **Annually** sign a nondisclosure statement and take this training
- Share data **only** with authorized survey team members
- **Refer** other requests for data access to the NAHMS study coordinator
- **Protect at all times** the confidential records- in whatever form or media- which are under your control

All persons granted access to confidential data will receive the NAHMS data confidentiality handbook. If you have any questions regarding confidentiality please refer to the handbook or contact the NAHMS Director.



Your Responsibilities



DON'T

- Mail, fax, or send confidential material without observing strict security procedures
- Discuss in public any identified person's or institution's participation in a survey
- Leave confidential records in places visible to unauthorized persons, such as a desk or vehicle
- Prepare or maintain unneeded copies of confidential material

Your Responsibilities



DON'T

- Remove confidential documents or files from NAHMS offices for any purpose (including taking them home to work on laptops, CDs, or flash drives) or access them electronically from an unauthorized remote location
 - Data collection agents may remove confidential information from offices in order to conduct surveys. All confidential information must be safeguarded appropriately while outside of the office

More Information

- *Privacy Act of 1974 (5 U.S.C. 552a)*
<http://www.justice.gov/opcl/privacyact1974.htm>
- CIPSEA, Title V of E-Gov Act of 2002 (Public Law 107–347, Dec. 17 2002):
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/info reg/cipsea/cipsea_statute.pdf
- OMB Implementing Guidelines (Federal Register Vol 72, No 115, June 15, 2007)
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/fedreg/2007/061507_cipsea_guidance.pdf
- OMB guides for a statistical agency:
http://www.whitehouse.gov/omb/inforeg_statpolicy
- Standards and Guides for Statistical Surveys:
http://www.whitehouse.gov/omb/assets/omb/inforeg/statpolicy/standards_stat_surveys.pdf

Summary:

- Confidentiality training is an annual requirement
- Protecting identifiable and confidential data is the law
- Disclosure of confidential data can lead to severe fines, imprisonment, or both
- Know your role and what you are required to do to keep data confidential