Chapter 5

Ethical Issues in Surveys

Eleanor Singer
Survey Research Center, Institute for Social Research
University of Michigan

ADDITIONAL WEB MATERIAL

The following additional material is listed in Chapter 5 of *The International Handbook of Survey Methodology*. It refers to section 5.5.7.c. *'What should researchers do to protect confidentiality?'*

Principles and Practices for Research Staff of the University of Michigan ISR Standing Committee on Confidentiality and Data Security (Chapter 5, section 5.5.7.c)

Example of the Confidentiality procedures of the Social and Economic Sciences Research Center (SESRC) of Washington State University (Chapter 5, section 5.5.7.c)

Example of Generic Confidentiality pledge for interviewers and other employees (Chapter 5, section 5.5.7.c)

Principles and Practices for Research Staff of the University of Michigan ISR Standing Committee on Confidentiality and Data Security (Chapter 5, section 5.5.7.c)

PROTECTION OF SENSITIVE DATA: Principles and Practices for Research Staff

The ISR Standing Committee on Confidentiality and Data Security of the University of Michigan, Ann Arbor, USA

From the April 1999 issue of the Center Survey, a newsletter for the staff of the Survey Research Center, Ann Arbor, MI. Courtesy ISR, University of Michigan

All ISR employees have signed a pledge to maintain the confidentiality of respondents' data, whether those are stored electronically or on paper questionnaires, audiotapes, or videotapes. Failure to adhere to this pledge could result in disciplinary action up to or including dismissal. This document describes some common principles of data security and specific practices that can be used to implement these principles.

1. Evaluate Risks

Any security measure must be assessed in the context of costs and benefits, both monetary and non-monetary. In applying the practices described below, weigh the time and effort required along with the sensitivity of the information protected. Electronic files, questionnaires, audiotapes or videotapes containing plain-text names and addresses of respondents to sensitive surveys certainly require a great deal of care in handling. Files containing edited and aggregated data may or may not need to be treated as confidential.

2. Assess the Sensitivity of All Data under Your Control

It is the responsibility of the staff member to determine the level of sensitivity of a particular file, document, or piece of E- mail. If you are in doubt, be conservative and seek the advice of your supervisor.

3. Apply Appropriate Security Measures

Interview-or self-administered questionnaires, whether stored on paper or electronic files, should not include identifying personal information such as full names, addresses, phone numbers, Social Security numbers, or other similar identifying information. The same is true of audiotapes and videotapes. Questionnaires or tapes containing personally sensitive information, for example about drug use or medical conditions, should be stored in locked cabinets. The same is true when the questionnaires

include responses to open-ended questions that may reveal the identity of the respondent or others.

4. Do Not Include Identifying Personal Information on Self-administered Questionnaires

If full names, addresses, phone numbers, Social Security numbers, or other similar identifying information is needed about the respondents or their close ones (family members, contact persons), provide a separate return envelope and ask them to mail back the identifying personal information separately from the questionnaire. Of thousands of questionnaires that are mailed back, it is reasonable to expect that a few may be damaged or otherwise opened on their journey back to the ISR. Separating identifying personal information is intended to eliminate the risk that accidental rupture or opening of a mailed envelope will result in a breach of confidentiality.

5. Store Cover Sheets with Personal Information about Respondents in Locked Cabinets

The lock should be unique to the cabinet, not the S-100 or a similar common lock. Do not leave questionnaires or cover sheets unattended. When these materials are being processed in open bay areas, they need to remain under the watchful supervision of an ISR employee until they are returned to their designated storage place.

6. Physically Secure Your Electronic Files as You Do Their Paper Copies

If paper files are sensitive enough to require storage in locked files, then the hard disks, floppies, or tapes containing electronic copies of these files require the same level of physical security. If you would not leave a list of respondents' names and addresses in an unlocked drawer, you should not leave floppy disk or a backup tape containing that list in an unlocked drawer. Consider keeping sensitive material on removable media (and NOT stored in unsecure locations of the network directory) which can be locked away (floppies, tapes, Zip disks, etc.).

7. Take Special Care to Secure Hard Disks Containing Sensitive Material

Personal computers (especially laptops) are popular targets for thieves. If sensitive material is on your local hard drive, there is a risk that it could be exposed if the machine is stolen. It is prudent to keep intrinsically valuable computing equipment containing sensitive information under tighter physical control than you would paper copies of the same information. Computers containing sensitive information should at minimum be kept in locked offices. Lock-down cables or enclosures that attach equipment to furniture may be appropriate. Laptops should be kept in locked drawers or cabinets. Close and lock your door when you are not in your office.

8. Segregate Sensitive Material from Non-sensitive Material
Label disks, tapes, and computers that contain confidential material so that other staff will know special care is needed in handling them. Keep sensitive files in a separate folder or partition on your hard disk so that you can easily back them up separately.

9. Consider Encryption of Sensitive Material
Encrypted files can be stored and backed up relatively freely even if they contain sensitive data. Encryption is a good practice when sensitive material must be transferred over the Internet (or any public network). However, be aware that maintaining encrypted files involves another set of risks: If the encryption key is forgotten, the original file is probably not recoverable; if the encryption key is compromised (or too easy to guess), the confidentiality may be breached. Contact your computer support staff to learn what encryption software is available for your use.

10. Recognize that Security Measures Have Costs as Well as Benefits
Routine backups of data files protect the investment of effort that went into creating them, but add to the risk that copies may fall into unauthorized hands. If some of your files are backed up on the network server, make sure they are appropriately protected.

11. Know the Physical Location of Your Electronic Files
Every electronic file has at least one physical representation, and often has many. An E-mail message may exist as a file on the hard disk of the sender's computer. It may be automatically stored in a folder of outgoing messages when it is sent. While it is in transit it may exist as packets of information traveling over a network as well as temporary files on intermediate mail servers on the Internet. When it arrives it may exist as a file on a local networked mail server as well as a file on your local hard drive. You may keep a copy on a removable disk or on paper. Any of these files might appear on system backup tapes. (Although it is standard practice for mail system administrators not to retain backups of electronic mail systems for more than seven days, copies saved on a backed-up file system may be retained indefinitely.)

12. Know the Backup Status of All Storage Systems You Use
Any security measures you take to protect confidential material needs to be applied to all copies of that material. This is not meant to imply that sensitive material should not be backed up, just that copies must be treated with the same level of care as the original files.

13. Be Aware that Electronic Mail Can Be Observed in Transit
Think of an E-mail message as though it were written on a postcard. Although it is impolite to read a postcard addressed to someone else, and although it is against Post Office policy for letter carriers to read them, it

is unwise to use postcards--or E-mails--for highly confidential communications.

14. Take Care When You Erase Files

In most cases, data which has been “erased” from floppies, hard disks, or tapes can be recovered. You need to overwrite the files to make sure that they will not be available to anyone with a file recovery program. You may want to reformat disks that have contained particularly sensitive material to ensure that it cannot be recovered. Similar care is needed when disposing of your computer. If you are unsure of what is required, get help from the computing staff.

Example of the Confidentiality procedures of the Social and Economic Sciences Research Center (SESRC) of Washington State University (Chapter 5, section 5.5.7.c)

SESRC CONFIDENTIALITY PROCEDURES
By courtesy of the Social and Economic Sciences Research Center, Washington State University, Pullman, USA

All surveys undertaken by the SESRC are reviewed for protection of human subjects by the Washington State University, Human Subjects Institutional Review Board (IRB). Survey procedures for ensuring confidentiality, rights to privacy, and consent to participate, must be reviewed by the IRB prior to the start of any interviews or mailing of questionnaires. In developing survey procedures, the SESRC follows the code of professional ethics and practices of the American Association for Public Opinion Research. That code states that "Unless the respondent waives confidentiality for specified uses, we shall hold as privileged and confidential all information that might identify a respondent with his or her responses. We shall also not disclose or use the names of respondents for non-research purposes unless the respondents grant us permission to do so."

The SESRC also follows the Code of Standards for Survey Research of the Council of American Survey Research Organizations. This code identifies two exceptions to the policy of not releasing respondent-identifying information to clients (1) when that information is needed to validate interviews, and (2) when it is used to determine additional facts of analytical importance to the study. In these latter two instances, the client must confirm in writing that they will respect and maintain respondent confidentiality before any confidential information is disclosed by the SESRC. Additionally, respondents must be informed, prior to or at the time of the interview or questionnaire, that clients will have access to respondent-identifying information.

Confidentiality Form Signed by SESRC Interviewing/Clerical Staff

Statement of Professional Ethics

All interviewers and other employees of the Social and Economic Sciences Research Center are expected to understand that their professional activities are directed and regulated by the following statements of policy.

Social and Economic Sciences Research Center Obligations
The rights of human subjects are a matter of primary concern to the Center. All study procedures are reviewed to ensure that individual respondents are protected at each stage of research. While it is the Center's policy to disseminate research results, the utmost care is taken to ensure that no data are released that would permit any respondent to be identified. All information that links a specific respondent to a particular interview is separated from the interview and put into special, secure files as soon as the interview is received and logged in at the Center. The interviews themselves are identified only by numbers.

Interviewer Obligations
The only acceptable role for an interview is that of a professional researcher. To depart from this role may introduce bias and compromise research objectives. In no case is an interviewer to attempt to counsel a respondent or sell any goods or services to a respondent or enter into any but a professional relationship with a respondent. If asked for help by a respondent, interviewers must limit themselves to providing the names of regular, recognized agencies and are to do this only when such information or help is specifically requested by the respondent. By the same token, no interviewer should ever ask for advice or counseling from a respondent or in any way exploit the research situation for personal advantage.

The respondent protection procedures observed by the Center will be undermined if interviewers do not maintain professional ethical standards of confidentiality regarding what they learn from or about respondents. All information obtained during the course of the research which concerns respondents, their families, or the organizations they represent, is privileged information whether it relates to the interview itself or is extraneous information leaned by interviewers during the performance of their work.

We have an obligation to respondents to keep their interviews confidential. We feel very strongly that this obligation should be honored. Therefore, please do not tell anyone the substance of any interview or part of an interview, no matter how fascinating or interesting it was. Also, please avoid giving your own summary of findings. Just because 90% of your respondents feel a certain way does not mean that 90% of everyone else feels the same way. Confidentiality is essential. Please help us maintain the reputation we have established for protecting anonymity of respondents, and honestly analyzing and reporting data. If you want a copy of results from this survey, let the supervisor know and we will be sure you get them just as soon as they are available.

Pledge of Confidentiality

The Social and Economic Sciences Research Center of Washington State University promises respondents that data will be kept completely confidential. We feel this obligation strongly and ask that all of our employees read the Statement of Professional Ethics and sign a Pledge of Confidentiality. Please read the statement on the back of this page carefully and sign this sheet to indicate that you understand and pledge to uphold the Center's policy of confidentiality.

Please sign your name and the date and print your name on the lines below.

_____ _____

Signature Date

_____ (PLEASE PRINT)

First Name Middle Initial Last Name

Example of Generic Confidentiality pledge for interviewers and other employees (Chapter 5, section 5.5.7.c)

Generic Confidentiality Form to be Signed by Interviewing/Clerical/Research Staff
Courtesy of SESRC, Washington State University, Pullman, USA

Statement of Professional Ethics

All interviewers and other employees of the Research Center are expected to understand that their professional activities are directed and regulated by the following statements of policy.

Research Center Obligations
The rights of human subjects are a matter of primary concern to the Research Center. All study procedures are reviewed to ensure that individual respondents are protected at each stage of research. While it is the Research Center's policy to disseminate research results, the utmost care is taken to ensure that no data are released that would permit any respondent to be identified. All information that links a specific respondent to a particular interview is separated from the interview and put into special, secure files as soon as the interview is received and logged in at the Research Center. The interviews themselves are identified only by numbers.

Interviewer Obligations
The only acceptable role for an interviewer is that of a professional researcher. To depart from this role may introduce bias and compromise research objectives. In no case is an interviewer to attempt to counsel a respondent or sell any goods or services to a respondent or enter into any but a professional relationship with a respondent. If asked for help by a respondent, interviewers must limit themselves to providing the names of regular, recognized agencies and are to do this only when such information or help is specifically requested by the respondent. By the same token, no interviewer should ever ask for advice or counseling from a respondent or in any way exploit the research situation for personal advantage.

The respondent protection procedures observed by the Research Center will be undermined if interviewers do not maintain professional ethical standards of confidentiality regarding what they learn from or about respondents. All information obtained during the course of the research which concerns respondents, their families, or the organizations they represent, is privileged information whether it relates to the interview itself or is extraneous information leaned by interviewers during the performance of their work.

We have an obligation to respondents to keep their interviews confidential. We feel very strongly that this obligation should be honored. Therefore, please do not tell anyone the substance of any interview or part of an interview, no matter how fascinating or interesting it was. Also, please avoid giving your own summary of findings. Just because 90% of your respondents feel a certain way does not mean that 90% of everyone else feels the same way. Confidentiality is essential. Please help us maintain the reputation we have established for protecting anonymity of respondents, and honestly analyzing and reporting data. If you want a copy of results from this survey, let the supervisor know and we will be sure you get them just as soon as they are available.

Pledge of Confidentiality

The Research Center promises respondents that data will be kept completely confidential. We feel this obligation strongly and ask that all of our employees read the Statement of Professional Ethics and sign a Pledge of Confidentiality. Please read the statement on the back of this page carefully and sign this sheet to indicate that you understand and pledge to uphold the Center's policy of confidentiality.

Please sign your name and the date and print your name on the lines below.

_____ _____

Signature Date

_____ (PLEASE PRINT)

First Name Middle Initial Last Name