

**CODE OF STANDARDS AND ETHICS
FOR SURVEY RESEARCH**

The Voice and Values of Research
CASRO[®]
COUNCIL OF AMERICAN SURVEY RESEARCH ORGANIZATIONS[®]

Council of American Survey Research Organizations[®] (CASRO[®])
170 North Country Road, Suite 4
Port Jefferson, New York 11777 USA
(631) 928-6954 • Fax: (631) 928-6041
www.casro.org • email: casro@casro.org

©1997 - 2008 CASRO - Council of American Survey Research Organizations. All Rights Reserved. First Adopted 1977. Revised as needed. This document is protected under the copyright laws of the United States and other countries and may not be reprinted or reproduced without permission from CASRO, provided that it may be referenced and quoted with attribution and credit given to CASRO.

TABLE OF CONTENTS

Introduction	4
I. Responsibilities to Respondents	5
II. Responsibilities to Clients	15
III. Responsibilities in Reporting to Clients and the Public	16
IV. Responsibilities to Outside Contractors and Interviewers	18
Appendix: Personal Data Classification	19

Addendums (for CASRO Members Only)

Found on Members Only section of CASRO website:

1. Standards regarding disclosure of respondent-identifiable data to clients
(Suggested Client Agreement)
2. Suggested CASRO Client Certification of Email Sample List Compliance

INTRODUCTION

This Code of Standards and Ethics for Survey Research sets forth the agreed upon rules of ethical conduct for Survey Research Organizations. Acceptance of this Code is mandatory for all CASRO® Members.

The Code has been organized into sections describing the responsibilities of a Survey Research Organization to Respondents, Clients and Outside Contractors and in reporting study results.

This Code is not intended to be, nor should it be, an immutable document. Circumstances may arise that are not covered by this Code or that may call for modification of some aspect of this Code. The Standards Committee and the Board of Directors of CASRO® will evaluate these circumstances as they arise and, if appropriate, revise the Code. The Code, therefore, is a living document that seeks to be responsive to the changing world of Survey Research. To continue to be contemporary, CASRO® advocates ongoing, two-way communication with Members, Respondents, Clients, Outside Contractors, Consultants and Interviewers.

Please also refer to other CASRO® Publications, which may provide detail relevant to many sections of the CASRO® *Code of Standards and Ethics for Survey Research*.

I. RESPONSIBILITIES TO RESPONDENTS

Preamble

Researchers have professional and legal responsibilities to their respondents that are embodied in the procedures of a research study. Underlying these specific responsibilities are four fundamental ethical principles:

Respondents should be:

- a. willing participants in survey research;
- b. appropriately informed about the survey's intentions and how their personal information and survey responses will be used and protected;
- c. sufficiently satisfied with their survey experience;
- d. willing to participate again in survey research.

A. Confidentiality

1. Since individuals who are interviewed are the lifeblood of the Survey Research Industry, it is essential that Survey Research Organizations be responsible for protecting from disclosure to third parties—including Clients and members of the Public—the identity of individual Respondents as well as Respondent-identifiable information, unless the Respondent expressly requests or permits such disclosure.
2. This principle of confidentiality is qualified by the following exceptions:
 - a. A minimal amount of Respondent-identifiable information will be disclosed to the Client to permit the Client: (1) to validate interviews and/or (2) to determine an additional fact of analytical importance to the study (including the practice of appending Client-owned database information to the Survey Research Organization's data file as an analytic aid). Where additional inquiry is indicated, Respondents must be given a sound reason for the re-inquiry; a refusal by Respondent to continue must be respected.

Before disclosing Respondent-identifiable information to a Client for purposes of interview validation or re-inquiry, the Survey Research Organization must take whatever steps are needed to ensure that the Client will conduct the validation or recontact in a fully professional manner. This includes the avoidance of multiple validation contacts or other conduct that would harass or could embarrass Respondents. It also includes avoidance of any use of the information (e.g., lead generation) for other than legitimate and ethical Survey Research purposes or to respond to Customer/Respondent complaints. Assurance that the Client will respect such limitations and maintain Respondent confidentiality should be confirmed in writing before any confidential information is disclosed.

Where Respondent-identifiable data is disclosed to clients so that the Survey Research Organization may analyze survey data in combination with other respondent-level data such as internal customer data, respondent-level data from another survey, etc., it is understood that the information will be used for

model building, internal (Survey Research Organization) analysis, or the like and not for individual marketing efforts and that **no action can be taken toward an individual respondent** simply because of his or her participation in the survey. To assure Client compliance, the Survey Research Organization must obtain written confirmation from the Client before releasing any data. (A suggested CASRO® Client agreement clause is available.)

Further, with respect to such research uses as Database Segmentation and/or Modeling (see preceding paragraph), specific action(s) may not be taken toward an **individual Respondent** as a result of his/her survey information and participation beyond those actions taken toward the **entire database population group** the Respondent **by chance** has been selected to represent. In order for such specific action, the following two elements must be met:

The Respondent has first given his/her permission to do so, having been told the **general purpose and limitations** of such use; and

The research firm has obtained **a written agreement from the Client** assuring that no other use will be made of Respondent-identifiable information.

Predictive equations which integrate a segmentation scheme into a Client database may be applied so long as **no action is taken toward an individual Respondent** simply because of his or her participation in the survey. Respondents must be treated like all other individuals in the database according to the segment(s) to which they belong or have been assigned.

- b. The identity of individual Respondents and Respondent-identifiable information may be disclosed to other Survey Research Organizations whenever such organizations are conducting different phases of a multi-stage study (e.g., a trend study). The initial Research Company should confirm in writing that Respondent confidentiality will be maintained in accordance with the Code.
 - c. In the case of research in which representatives of the Client or others are present, such Client representatives and others should be asked not to disclose to anyone not present the identity of individual Participants or other Participant-identifying information except as needed to respond, with the Participant's prior specific approval, to any complaint by one or more of the Participants concerning a product or service supplied by the Client.
3. The principle of Respondent confidentiality includes the following specific applications or safeguards:
- a. Survey Research Organizations' staff or personnel should not use or discuss Respondent-identifiable data or information for other than legitimate internal research purposes.
 - b. The Survey Research Organization has the responsibility for insuring that Subcontractors (Interviewers, Interviewing Services and Validation, Coding, and Tabulation Organizations) and Consultants are aware of and agree to maintain and respect Respondent confidentiality whenever the identity of Respondents or Respondent-identifiable information is disclosed to such entities.

-
- c. Before permitting Clients or others to have access to completed questionnaires in circumstances other than those described above, Respondent names and other Respondent-identifying information (e.g., telephone numbers) should be deleted.
 - d. Invisible identifiers on mail questionnaires that connect Respondent answers to particular Respondents should not be used. Visible identification numbers may be used but should be accompanied by an explanation that such identifiers are for control purposes only and that Respondent confidentiality will not be compromised.
 - e. Any Survey Research Organization that receives from a Client or other entity information that it knows or reasonably believes to be confidential, Respondent-identifiable information should only use such information in accordance with the principles and procedures described in this Code.
 - f. The use of survey results in a legal proceeding does not relieve the Survey Research Organization of its ethical obligation to maintain in confidence all Respondent-identifiable information or lessen the importance of Respondent anonymity. Consequently, Survey Research firms confronted with a subpoena or other legal process requesting the disclosure of Respondent-identifiable information should take all reasonable steps to oppose such requests, including informing the court or other decision-maker involved of the factors justifying confidentiality and Respondent anonymity and interposing all appropriate defenses to the request for disclosure.

B. Privacy and the Avoidance of Harassment

1. Survey Research Organizations have a responsibility to strike a proper balance between the needs for research in contemporary American life and the privacy of individuals who become the Respondents in the research. To achieve this balance:
 - a. Respondents will be protected from unnecessary and unwanted intrusions and/or any form of personal harassment.
 - b. The voluntary character of the Interviewer-Respondent contact should be stated explicitly where the Respondent might have reason to believe that cooperation is not voluntary.
2. This principle of privacy includes the following specific applications:
 - a. The Research Organization, Subcontractors and Interviewers shall make every reasonable effort to ensure that the Respondent understands the purpose of the Interviewer/Respondent contact.
 - (1) The Interviewer/Research Company representative must provide prompt and honest identification of his/her research firm affiliation.
 - (2) Respondent questions should be answered in a forthright and non-deceptive manner.

-
- b. Deceptive practices and misrepresentation, such as using research as a guise for sales or solicitation purposes, are expressly prohibited.
 - c. Survey Research Organizations must respect the right of individuals to refuse to be interviewed or to terminate an interview in progress. Techniques that infringe on these rights should not be employed, but Survey Research Organizations may make reasonable efforts to obtain an interview including:
 - (1) explaining the purpose of the research project;
 - (2) providing a gift or monetary incentive adequate to elicit cooperation; and
 - (3) re-contacting an individual at a different time if the individual is unwilling or unable to participate during the initial contact.
 - d. Research Organizations are responsible for arranging interviewing times that are convenient for respondents.
 - e. Lengthy interviews can be a burden. Research Organizations are responsible for weighing the research need against the length of the interview and Respondents must not be enticed into an interview by a misrepresentation of the length of the interview.
 - f. Research Organizations are responsible for developing techniques to minimize the discomfort or apprehension of Respondents and Interviewers when dealing with sensitive subject matter.
 - g. Electronic equipment (taping, recording, photographing) and one-way viewing rooms may be used only with the full knowledge of Respondents.

3. Internet Research

The unique characteristics of Internet research require specific notice that the principle of respondent privacy applies to this new technology and data collection methodology. The general principle of this section of the Code is that survey Research Organizations will not use unsolicited emails to recruit survey respondents or engage in surreptitious data collection methods. This section is organized into three parts:

a. email solicitations, b. active agent technologies, and c. panel/sample source considerations.

a. Email Solicitation

- (1) Research Organizations are required to verify that individuals contacted for research by email have a reasonable expectation that they will receive email contact for research. Such agreement can be assumed when ALL of the following conditions exist:
 - (a) A substantive pre-existing relationship exists between the individuals contacted and the Research Organization, the Client supplying email addresses, or the Internet Sample Providers supplying the email addresses (the latter being so identified in the email invitation);
 - (b) Survey email invitees have a reasonable expectation, based on the pre-existing relationship where survey email invitees have specifically opted in for Internet research with the research company or Sample Provider, or in the case of Client-supplied lists that they may be contacted for research and invitees have not opted out of email communications;

-
- (c) Survey email invitations clearly communicate the name of the sample provider, the relationship of the individual to that provider, and clearly offer the choice to be removed from future email contact.
 - (d) The email sample list excludes all individuals who have previously requested removal from future email contact in an appropriate and timely manner.
 - (e) Participants in the email sample were not recruited via unsolicited email invitations.
- (2) Research Organizations are prohibited from using any subterfuge in obtaining email addresses of potential respondents, such as collecting email addresses from public domains, using technologies or techniques to collect email addresses without individuals' awareness, and collecting email addresses under the guise of some other activity.
 - (3) Research Organizations are prohibited from using false or misleading return email addresses or any other false and misleading information when recruiting respondents. As stated later in this Code, Research Organizations must comply with all federal regulations that govern survey research activities. In addition, Research Organizations should use their best efforts to comply with other federal regulations that govern unsolicited email contacts, even though they do not apply to survey research.
 - (4) When receiving email lists from Clients or Sample Providers, Research Organizations are required to have the Client or Sample Provider verify that individuals listed have a reasonable expectation that they will receive email contact, as defined, in (1) above.
 - (5) The practice of "blind studies" (for sample sources where the sponsor of the study is not cited in the email solicitation) is permitted if disclosure is offered to the respondent during or after the interview. The respondent must also be offered the opportunity to "opt-out" for future research use of the sample source that was used for the email solicitation.
 - (6) Information about the CASRO Code of Standards and Ethics for Survey Research should be made available to respondents.

b. Active Agent Technology

- (1) Active agent technology is defined as any software or hardware device that captures the behavioral data about data subjects in a background mode, typically running concurrently with other activities. This category includes tracking software that allows Research Organizations to capture a wide array of information about data subjects as they browse the Internet. Such technology needs to be carefully managed by the research industry via the application of research best practices.

Active agent technology also includes direct to desktop software downloaded to a user's computer that is used solely for the purpose of alerting potential survey respondents, downloading survey content or asking survey questions. A direct to desktop tool does not track data subjects as they browse the Internet and all data collected is provided directly from user input.

Data collection typically requires an application to download onto the subjects' desktop, laptop or PDA (including personal wireless devices). Once downloaded, tracking software has the capability of capturing the data subject's actual experiences when using the Internet such as Web page hits, web pages visited, online transactions completed, online forms completed, advertising click-through rates or impressions, and online purchases.

Beyond the collection of information about a user's Internet experience, the software has the ability to capture information from the data subject's email and other documents stored on a computer device such as a hard disk. Some of this technology has been labeled "spyware," especially because the download or installation occurs without the data subject's full knowledge and specific consent. The use of spyware by a member of CASRO is strictly prohibited.

A cookie (defined as a small amount of data that is sent to a computer's browser from a web server and stored on the computer's hard drive) is not an active agent. The use of cookies is permitted if a description of the data collected and its use is fully disclosed in a Research Organizations' privacy policy.

- (2) Following is a list of unacceptable practices that Research Organizations should strictly forbid or prevent. A Research Organization is considered to be using spyware when it fails to adopt all of the practices in set forth in Section 3 below or engages in any in the following practices:
- (a) Downloading software without obtaining the data subject's informed consent.
 - (b) Downloading software without providing full notice and disclosure about the types of information that will be collected about the data subject, and how this information may be used. This notice needs to be conspicuous and clearly written.
 - (c) Collecting information that identifies the data subject without obtaining affirmed consent.
 - (d) Using keystroke loggers without obtaining the data subject's affirmed consent.
 - (e) Installing software that modifies the data subject's computer settings beyond that which is necessary to conduct research providing that the software doesn't make other installed software behave erratically or in unexpected ways.
 - (f) Installing software that turns off anti-spyware, anti-virus, or anti-spam software.
 - (g) Installing software that seizes control or hijacks the data subject's computer.
 - (h) Failing to make commercially reasonable efforts to ensure that the software does not cause any conflicts with major operating systems and does not cause other installed software to behave erratically or in unexpected ways.
 - (i) Installing software that is hidden within other software that may be downloaded.

-
- (j) Installing software that is difficult to uninstall.
 - (k) Installing software that delivers advertising content, with the exception of software for the purpose of ad testing.
 - (l) Installing upgrades to software without notifying users.
 - (m) Changing the nature of the active agent program without notifying user.
 - (n) Failing to notify the user of privacy practice changes relating to upgrades to the software.
- (3) Following are practices Research Organizations that deploy active agent technologies should adopt. Research Organizations that adopt these practices and do not engage in any of the practices set forth in Section 2 above will not be considered users of spyware.
- (a) Transparency to the data subject is critical. Research companies must disclose information about active agents and other software in a timely and open manner with each data subject. This communication must provide details on how the Research Organization uses and shares the data subject's information.
 - i. Only after receiving an affirmed consent or permission from the data subject or parent's permission for children under the age of 18, should any research software be downloaded onto the individual's computer or PDA.
 - ii. Clearly communicate to the data subject the types of data if any, that is being collected and stored by an active agent technology.
 - iii. Disclosure is also needed to allow the data subject to easily uninstall research software without prejudice or harm to them or their computer systems.
 - iv. Personal information about the subject should not be used for secondary purposes or shared with third parties without the data subject's consent.
 - v. Research Organizations are obligated to ensure that participation is a conscious and voluntary activity. Accordingly, incentives must never be used to hide or obfuscate the acceptance of active agent technologies.
 - vi. Research Organizations that deploy active agent technologies should have a method to receive queries from end-users who have questions or concerns. A redress process is essential for companies if they want to gauge audience reaction to participation on the network.
 - vii. On a routine and ongoing basis, consistent with the stated policies of the Research Organization, data subjects who participate in the research network should receive clear periodic notification that they are actively recorded as participants, so as to insure that their participation is voluntary. This notice should provide a clearly defined method to uninstall the Research Organization's tracking software without causing harm to the data subject.

-
- (b) Stewardship of the data subject is critical. Research companies must take steps to protect information collected from data subjects.
- i. Personal or sensitive data (as described in the Personal Data Classification Appendix) should not be collected. If collection is unavoidable, the data should be destroyed immediately. If destruction is not immediately possible, it: (a) should receive the highest level of data security and (b) should not be accessed or used for any purpose.
 - ii. Research Organizations have an obligation to establish safeguards that minimize the risk of data security and privacy threats to the data subject.
 - iii. It is important for Research Organizations to understand the impact of their technology on end-users, especially when their software downloads in a bundle with other comparable software products.
 - iv. Stewardship also requires the Research Organization to make commercially reasonable efforts to ensure that these “free” products are also safe, secure and do not cause undue privacy or data security risks.
 - v. Stewardship also requires a Research Organization that deploys active agent technologies to be proactive in managing its distribution of the software. Accordingly, companies must vigorously monitor their distribution channel and look for signs that suggest unusual events such as high churn rates.
 - vi. If unethical practices are revealed, responsible research companies should strictly terminate all future dealings with this distribution partner.

c. Panel/Sample Source Considerations

The following applies to all Research Organizations that utilize the Internet and related technologies to conduct research.

- (1) The Research Organization must:
 - (a) Disclose to panel members that they are part of panel.
 - (b) Obtain panelist’s permission to collect and store information about the panelist.
 - (c) Collect and keep appropriate records of panel member recruitment, including the source through which the panel member was recruited.
 - (d) Collect and maintain records of panel member activity.
- (2) Upon Client request, the Research Organization must disclose:

-
- (a) Panel composition information (including panel size, populations covered, and the definition of an active panelist).
 - (b) Panel recruitment practice information.
 - (c) Panel member activity.
 - (d) Panel incentive plans.
 - (e) Panel validation practices.
 - (f) Panel quality practices.
 - (g) Aggregate panel and study sample information (this information could include response rate information, panelist participation in other research by type and timeframe, see Responsibilities in Reporting to Clients and the Public).
 - (h) Study related information such as email invitation(s), screener wording, dates of email invitations and reminders, and dates of fieldwork.
- (3) Stewardship of the data collected from panelists is critical:
- (a) Panels must be managed in accordance with applicable data protection laws and regulations.
 - (b) Personal or sensitive data should be collected and treated as specified in the Personal Data Classification Appendix.
 - (c) Upon panelist request, the panelist must be informed about all personal data (relating to the panelist that is provided by the panelist, collected by an active agent, or otherwise obtained by an acceptable method specified in a Research Organization's privacy policy) maintained by the Research Organization. Any personal data that is indicated by panel member as not correct or obsolete must be corrected or deleted as soon as practicable.
- (4) Panel members must be given a straightforward method for being removed from the panel if they choose. A request for removal must be completed as soon as practicable and the panelist must not be selected for future research studies.
- (5) A privacy policy relating to use of data collected from or relating to the panel member must be in place and posted online. The privacy policy must be easy to find and use and must be regularly communicated to panelists. Any changes to the privacy policy must be communicated to panelists as soon as possible.
- (6) Research Organizations should take steps to limit the number of survey invitations sent to targeted respondents by email solicitations or other methods over the Internet so as to avoid harassment and response bias caused by the repeated recruitment and participation by a given pool (or panel) of data subjects.

-
- (7) Research Organizations should carefully select sample sources that appropriately fit research objectives and Client requirements. All sample sources must satisfy the requirement that survey participants have either opted-in for research or have a reasonable expectation that they will be contacted for research.
 - (8) Research Organizations should manage panels to achieve the highest possible research quality. This includes managing panel churn and promptly removing inactive panelists.
 - (9) Research Organizations must maintain survey identities and email domains that are used exclusively for research activities.
 - (10) If a Research Organization uses a sample source (including a panel owned by the Research Organization or a subcontractor) that is used for both survey research and direct marketing activities, the Research Organization has an obligation to disclose the nature of the marketing campaigns conducted with that sample source to Clients so that they can assess the potential for bias.
 - (11) All data collected on behalf of a Client must be kept confidential and not shared or used on behalf of another Client (see also Responsibilities to Clients).

II. RESPONSIBILITIES TO CLIENTS

- A. Relationships between a Survey Research Organization and Clients for whom the surveys are conducted should be of such a nature that they foster confidence and mutual respect. They must be characterized by honesty and confidentiality.
- B. The following specific approaches describe in more detail the responsibilities of Research Organizations in this relationship:
1. A Survey Research Organization must assist its Clients in the design of effective and efficient studies that are to be carried out by the Research Company. If the Survey Research Organization questions whether a study design will provide the information necessary to serve the Client's purposes, it must make its reservations known.
 2. A Research Organization must conduct the study in the manner agreed upon. However, if it becomes apparent in the course of the study that changes in the plans should be made, the Research Organization must make its views known to the Client promptly.
 3. A Research Organization has an obligation to allow its Clients to verify that work performed meets all contracted specifications and to examine all operations of the Research Organization that are relevant to the proper execution of the project in the manner set forth. While Clients are encouraged to examine questionnaires or other records to maintain open access to the research process, the Survey Research Organization must continue to protect the confidentiality and privacy of survey Respondents.
 4. When more than one Client contributes to the cost of a project specially commissioned with the Research Organization, each Client concerned shall be informed that there are other Participants (but not necessarily their identity).
 5. Research Organizations will hold confidential all information that they obtain about a Client's general business operations, and about matters connected with research projects that they conduct for a Client.
 6. For research findings obtained by the agency that are the property of the Client, the Research Organization may make no public release or revelation of findings without expressed, prior approval from the Client.
- C. Bribery in any form and in any amount is unacceptable and is a violation of a Research Organization's fundamental, ethical obligations. A Research Organization and/or its principals, officers and employees should never give gifts to Clients in the form of cash. To the extent permitted by applicable laws and regulations, a Research Organization may provide nominal gifts to Clients and may entertain Clients, as long as the cost of such entertainment is modest in amount and incidental in nature.

III. RESPONSIBILITIES IN REPORTING TO CLIENTS AND THE PUBLIC

- A. When reports are being prepared for Client confidential or public release purposes, it is the obligation of the Research Organization to insure that the findings they release are an accurate portrayal of the survey data, and careful checks on the accuracy of all figures are mandatory.
- B. A Research Organization's report to a Client or the Public should contain, or the Research Organization should be ready to supply to a Client or the Public on short notice, the following information about the survey:
1. The name of the organization for which the study was conducted and the name of the organization conducting it.
 2. The purpose of the study, including the specific objectives.
 3. The dates on or between which the data collection was done.
 4. A definition of the universe that the survey is intended to represent and a description of the population frame(s) that was actually sampled.
 5. A description of the sample design, including the method of selecting sample elements, method of interview, cluster size, number of callbacks, Respondent eligibility or screening criteria, and other pertinent information.
 6. A description of results of sample implementation including (a) a total number of sample elements contacted, (b) the number not reached, (c) the number of refusals, (d) the number of terminations, (e) the number of non-eligibles, (f) the number of completed interviews.
 7. The basis for any specific "completion rate" percentages should be fully documented and described.
 8. The questionnaire or exact wording of the questions used, including Interviewer directions and visual exhibits.
 9. A description of any weighting or estimating procedures used.
 10. A description of any special scoring, data adjustment or indexing procedures used. (Where the Research Organization uses proprietary techniques, these should be described in general and the Research Organization should be prepared to provide technical information on demand from qualified and technically competent persons who have agreed to honor the confidentiality of such information).
 11. Estimates of the sampling error and of data should be shown when appropriate, but when shown they should include reference to other possible sources of error so that a misleading impression of accuracy or precision is not conveyed.
 12. Statistical tables clearly labeled and identified as to questionnaire source, including the number of raw cases forming the base for each cross-tabulation.

-
13. Copies of Interviewer instructions, validation results, code books, and other important working papers.
- C. As a **minimum**, any general public release of survey findings should include the following information:
1. The sponsorship of the study.
 2. A description of the purposes.
 3. The sample description and size.
 4. The dates of data collection.
 5. The names of the research company conducting the study.
 6. The exact wording of the questions.
 7. Any other information that a lay person would need to make a reasonable assessment of the reported findings.
- D. A Survey Research Organization will seek agreements from Clients so that citations of survey findings will be presented to the Research Organization for review and clearance as to accuracy and proper interpretation prior to public release. A Research Organization will advise Clients that if the survey findings publicly disclosed are incorrect, distorted, or incomplete, in the Research Organization's opinion, the Research Organization reserves the right to make its own release of any or all survey findings necessary to make clarification.

IV. RESPONSIBILITIES TO OUTSIDE CONTRACTORS AND INTERVIEWERS

- A. Research Organizations will not ask any Outside Contractor or Interviewer to engage in any activity which is not acceptable as defined in other sections of this *Code of Standards and Ethics for Survey Research* or related CASRO® publications.

APPENDIX: PERSONAL DATA CLASSIFICATION

Classification Level Name	“Ordinary Personal Data” ¹	“Sensitive Personal Data” ²	“Hyper-Sensitive Personal Data” ³
Criteria	Data that is identifiable to an individual person but is not “Sensitive Personal Data.”	Data that is (1) identifiable to an individual person and (2) has the potential to be used to harm or embarrass the person.	Individually identifiable data that typically has no legitimate survey research value or purpose and has a very high potential to harm or embarrass the data subject.
Examples	Name Telephone # (work & home) Address (work & home) E-mail address (work and home) Internal Company ID numbers Gender Marital status # of Children Date of Birth, Age Citizenship Education Income range Veteran status Immigration status Languages spoken Country of residence Non-medical benefits information Purchase history, buying patterns, shopping patterns, hobbies All other personal data not “Sensitive Personal Data” IP address	Criminal arrests or convictions Judgments in civil cases Administrative sanctions Race, ethnicity, national origin Political opinions Religious or philosophical beliefs Union & Trade-union membership Data concerning health or medical treatment Data concerning sexual orientation or activity Financial data (such as credit rating, excluding items listed as Hyper-Sensitive Personal Data) Salary & Compensation Disability status	Social Security Numbers National ID Numbers Driver’s License # Financial Information (Credit card #s, Account #s) Passwords
Administrative Access Restrictions (e.g., access granted only to employees with a demonstrable need to know)	Access restricted to persons with a need to know for legitimate business purposes, and who have signed a confidentiality agreement.	Access restricted to persons with a need to know for legitimate business purposes, and who have signed a confidentiality agreement, and who have been specifically designated by management.	Do not collect if at all possible; implement processes to eliminate data that’s not used or ask client to provide only essential data. If collected and not eliminated do not disclose to third parties and apply the same Administrative Access requirements as Sensitive Personal Data.
Physical Labeling (e.g., papers and diskette or tape label)	“Personal Data” label in a conspicuous location on each document.	“Sensitive Personal Data” label in a conspicuous location on each document.	Same as Sensitive Personal Data.
Electronic Labeling (e.g., digital file, e-mail, or web page)	“Personal Data” label in a conspicuous location on each digital file, e-mail, or web page, and on subject line of messages.	“Sensitive Personal Data” label in a conspicuous location on each digital file, e-mail, or Web page, and on subject line of messages.	Same as Sensitive Personal Data.

Classification Level Name	“Ordinary Personal Data” ¹	“Sensitive Personal Data” ²	“Hyper-Sensitive Personal Data” ³
Physical Storage (e.g., secure room, locked drawer)	Storage in a secure office or other location. Room need not be locked if access to the building or floor is restricted to persons who are authorized to see the data.	Storage in a locked drawer, file cabinet, or office required. If stored in an open-file storage area, access to the area must be restricted to persons who are authorized to see the data.	Same as Sensitive Personal Data.
Electronic Storage (e.g., password protection, encryption)	Stored in a directory or folder with restricted access, e.g., password protection.	Stored in a directory or folder with restricted access, e.g., password protection.	Same as Sensitive Personal Data.
Physical Transmission (e.g., sealed envelope, bonded courier)	Sealed envelope.	Sealed double envelopes with bonded courier, and data encrypted with minimum 128 bit key.	Same as Sensitive Personal Data.
Electronic Transmission (e.g., encrypted, authentication of recipient)	Information should be transmitted to a verified account (email address or login ID).	Information should be transmitted to a verified account (email address or login ID) and the data should be transmitted in encrypted form (minimum 128-bit key).	Same as Sensitive Personal Data.
Physical Disposal (e.g., shredding of paper or other media)	After applicable Electronic Disposal, secure onsite disposal (including shredding of paper).	After applicable Electronic Disposal, secure onsite disposal (including shredding of paper). Disposal audit trail required.	Same as Sensitive Personal Data.
Electronic Disposal (e.g., wiping of disk, degaussing)	Where feasible and possible, removal of directory entry for file, and overwriting of file space with other data. Alternatively, security certification where data becomes embedded in archives and cannot be selectively deleted.	Where feasible and possible, degaussing (wiping) of media or physical destruction of media. Alternatively, security certification where data becomes embedded in archives and cannot be selectively degaussed (wiped).	Same as Sensitive Personal Data.

¹ Standard demographic data included in surveys are only considered “Ordinary Personal Data” if it is identifiable to an individual person.

² Standard demographic data included in surveys are only considered “Sensitive Personal Data” if it is identifiable to an individual person. It may be necessary to create additional classification levels for data that is subject to specific statutory requirements, such as “personal health information” subject to HIPAA.

³ It may be necessary to create additional classification levels for data that is subject to specific statutory requirements, such as “personal health information” subject to HIPAA.

For more information about



CODE OF STANDARDS AND ETHICS FOR SURVEY RESEARCH

please visit

www.casro.org

or contact

Council of American Survey Research Organizations® (CASRO®)
170 North Country Road, Suite 4
Port Jefferson, New York 11777 USA
(631) 928-6954 • Fax: (631) 928-6041
email: casro@casro.org



© CASRO, 2008

www.casro.org