THE UNIVERSITY OF CHICAGO
SURVEY LAB
DIVISION OF THE SOCIAL SCIENCES

Data Security Statement

As part of the Division of the Social Sciences at the University of Chicago, the Survey Lab conducts research to increase general knowledge, improve public policy, train the next generation of social scientists and improve social science data collection methods. We collect data for academic, non-profit and government clients. To preserve our role in knowledge creation, results of studies for which we collect data should be on track for eventual publication in a journal or newsletter, on a webpage, or in some other form that would be accessible to the public. We do not collect proprietary data intended for private use by for-profit entities.

Respondent confidentiality

Data that we collect is always subject to the rules of confidentiality set out at the start of each study by one of the University of Chicago Institutional Review Boards (IRB), bodies at the University that protect the rights of persons who participate in research. No results may be shared that link individual respondent identities to the content of the data they supplied unless respondents agree to this and our IRB approves it. Normally the Survey Lab will maintain all identifying and contact information required for data collection separately from the data themselves, and will destroy contact information at the end of the data collection period. Exceptions include contact information retained over time for longitudinal studies, information retained at the request of the respondent for participation in future studies, and contact information related to receipts and accounting that has no link to individual studies. We typically supply clients with data separated from individual contact information. Respondent information may be shared with clients depending on arrangements made in advance with our IRB and with any IRB committees to which our clients may report.

Training and oversight

Staff members are trained in the protection of human subjects in research and the importance of preserving the confidentiality of all respondents in all data collection. This is a commitment we take very seriously. Full-time staff members maintain IRB training certification through the online Collaborative Institutional Training Initiative (CITI) program. In addition to general and project-specific training for maintaining research participant confidentiality, all staff members, contractors and visitors must sign a pledge that commits them to vigilant protection of the privacy of research subjects. Research assistants are supervised closely by permanent staff and reminded regularly of confidentiality precautions. All persons not employed directly by the Survey Lab, including building security and cleaning staff, are only allowed in our space when accompanied by a staff person.

Dis-identification

When we conduct focus groups, interviews, observational work or qualitative work including transcriptions or field notes, notes and transcripts are dis-identified. This means that names are not associated with responses and that references to named people, places or things that might identify a participant are removed or made "generic" (i.e. "Susan" may become "sister;" "Father George" may become "religious leader;" and "Northwestern Hospital" may become "Large teaching hospital").

Data on paper

Data collected on paper are stored in a locked room when not in current use. When projects are completed, contact information required for data collection but dissociated from data for confidentiality purposes is shredded or deleted.

Electronic data

Electronic data are kept in one or multiple the following secure systems:

1) A share drive on one of the servers maintained and serviced by the University's Social Sciences Computing support group. The Survey Lab maintains a meticulous organization of files on this share drive. Access to files is provided on a graduated basis, with higher levels of access reserved for those who need it and have been cleared by Survey Lab staff. Lower levels provide access only to general forms, project instruments and reference materials. Higher levels are reserved for sample-level data (containing attempt and contact information but no collected data) and collected data. We review our permissions list on a monthly basis or more often as needed to keep it up to date.

2) A server for implementing computer-assisted telephone interviewing (CATI) and web surveys, owned and used only by the Survey Lab, maintained and serviced by a server administrator in the Social Sciences Computing Support group. This server is housed in a room that is locked and alarmed when not in use by CATI staff.

   Data stored on the Survey Lab's web server are protected through two different sets of firewall rules that govern access to the server's public and private network adapters—each minimalized to its specific function. We employ a combination of a Microsoft-based firewall technology and the physical barrier of a Cisco RVS4000 4-port Gigabit Security Router installed between the server and its internet connection. The router uses NAT with port forwarding to restrict the types of network traffic that can reach the server from the internet. The only types of network traffic that the router passes to the server are https (SSL-encypted web traffic) and Windows Remote Desktop (limited by firewall rules to use for administrative purposes by a single Social Sciences Computing computer). Survey data transferred online use a TLS 1.0 connection with 128-bit encryption, using AES_128_CBC with SHA1 for message authentication and RSA as the key exchange mechanism.

   The server has a second network interface card that connects to a private non-routable and non-bridged network that consists of the interviewer workstations, which have no regular access to the internet or any other outside network. Access to the server from the workstations on the private network is limited to the minimum essential network services and minimal privileges required by Sawtooth software to run CATI interviews. Data on the server can be accessed from within the CATI Center at the Survey Lab, a room which is locked and alarmed when not in use. Both access in the CATI Center and access online through the Sawtooth software require a user name and password that are known only to study supervisors.

   We also use the Microsoft IIS outgoing SMTP mail server to send emails to respondents. It is configured to be accessible only to CATI center workstations on the private network; this restriction is accomplished both by the rules set in IIS as well as by the Windows Firewall rules.

3) The Survey Lab uses an online platform called Qualtrics (qualtrics.com) to field some online surveys. Qualtrics allows for more efficient programming and higher volume than can be achieved on our local server. Whenever possible, we do not upload any identifying information to Qualtrics, only unique IDs so that we can store all identifying information locally. Qualtrics maintains a high level of security, allows for SSL encryption, and is used by many university and government entities. See the web addresses below for more information about their security and privacy policies:

   Qualtrics security statement: http://www.qualtrics.com/security-statement
   Qualtrics privacy statement: http://www.qualtrics.com/privacy-statement