**Guide 613 - Internet-Based Research Guide**

*This guidance document is intended for researchers conducting recruitment, informed consent, and/or data collection activities over the internet. For additional assistance, please contact the UH Human Studies Program at 808-956-8287*

1. **Recruitment**
	1. Advertising and recruiting potential participants using the internet should follow the guidelines for recruitment that apply to any traditional media (e.g., flyers, newspaper ads).
		1. Examples of internet-based recruitment methods:
			* Email
			* Online Advertising
			* Chatroom Postings
		2. All recruitment materials must be submitted for review and approval before use in the field.
		3. ***Note:*** Per FDA guidance, prior IRB review is not necessary for general listings of clinical trials on websites that provides information limited to basic description information, including study title, purpose of the study, protocol summary, basic eligibility criteria, study site locations, and contact information for further information on the study.
		4. For Human Studies Program (HSP) guidelines on recruitment flyers: <https://manoa.hawaii.edu/researchcompliance/sites/manoa.hawaii.edu.researchcompliance/files/resource/Recruitment_Flyer_Guidelines.pdf>
	2. ***Beware***: The proper identification and qualification of subjects can be challenging to verify in internet-based research. In studies in which authentication of subjects is important to the validity of the data or that consist of a particularly sensitive topic, investigators should discuss measures taken to authenticate subjects.
		1. Strategies for authentication include, but not limited to:
			* Providing each study participant (in person or by U.S. Postal Service mail) with a Personal Identification Number (PIN) to be used for authentication in subsequent computer- and internet-based data collection. The PIN used, however, must not be one that could be used by others to identify the individual (e.g., social security number, phone number, birth date, etc.).
			* Minors may be screened by checking for internet monitoring using an adult verification system. This may be necessary if the study presents more than minimal risk to subjects or asks particularly sensitive questions. On the other hand, if the study involves not greater than minimal risk, the informed consent document may simply ask participants to confirm that they are the appropriate age for the research. The IRB will determine if risk is greater than minimal.
	3. **Research Participant Pools** are mutually beneficial systems that provide investigators easy access to a large set of potential research participants. Although the purpose of hosting a participant pool is to facilitate human subjects research, it is not subject to IRB review and approval since no personal data is collected. However, texts to advertise potential participants to join these pools should similarly follow the guideline for developing traditional recruitment media. Participant pools are often developed by a department within the university, and may be done in the following ways:
		1. ***Research management system:***  a web-based tool that allows potential participants log-in to a site that lists individually-approved research projects seeking research participants. Potential participants can “shop around” for research to participate, and at the conclusion of their participation are usually given extra credit as compensation (i.e., Sona Experiment Management System).
		2. ***Participant pool listserv:***  mass email may be sent out with the help of administrative departments, communicating to potential participants to register in a department-hosted participant pool. Individually-approved research projects from the hosting department are advertised by email to those potential participants who had registered to be included in this participant pool. Registrants may unsubscribe to this pool at any time.
2. **Informed Consent**
	1. When online surveys are being used, the HSP template for “Anonymous Survey Consent (Online)” may be adapted (<https://manoa.hawaii.edu/researchcompliance/templates>). Whether the study is exempt or non-exempt, consenting documents must include required elements of an informed consent. HSP guideline for informed consents can be found at <https://manoa.hawaii.edu/researchcompliance/policies-guidance>.
	2. ***Research involving minors:*** Generally, investigators conducting internet-based research with minors must obtain both child assent and parent permission. Researchers may request a waiver of parent permission provided the research fits the appropriate criteria, per 45 CFR 46.116(c) or (d), or 46.408(c) (<http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html#46.116>, <http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.html#46.408>).
	3. In order to utilize either of these two consent procedures, the investigator must request a waiver of documented consent to the IRB.
		1. The use of “I agree” or “I do not agree” buttons (or other electronic methods for indicating affirmative consent) on online pages in lieu of signatures is acceptable.
		2. For surveys sent to and returned by participants through email, investigators should include a consent document and inform participants that submitting the completed survey indicates their consent.
	4. The process of requesting consent should not disrupt normal group activity. Researchers need to be particularly sensitive of this when entering online communities and chatrooms as the process of requesting consent is often perceived as disruptive. If seeking informed consent will harm the validity of a study or make the research impracticable, it may be possible to obtain a waiver of consent provided the study meets the appropriate criteria. When requesting a waiver of informed consent, issues regarding deception or incomplete disclosure must be addressed in the researcher’s application.
	5. Personas, or avatars, are social identities that internet users establish in online communities and websites. These personas allow individuals to reveal varying levels of personal information and also allow them to navigate the virtual world as a particular character or alter-ego. Names of internet personas (characters or avatars) or real names may be used in reports and publications only with consent from the participating individual. (see Data Security below for more information). ***In these situations, specific language concerning the release of identifiable information must be included in the informed consent document and specific consent must be sought from subjects for this release.***  If research participants give consent to be identified, data must still be secured properly to avoid any misuse by a third party.
	6. Collecting data over the internet can increase potential risks to confidentiality because of the frequent involvement of third party sites and the risk of third party interception when transmitting data across a network e.g., automatic serve logs and backups). Additionally, third party sites may have their own security measures that do not match those of the investigators’. Participants should be informed of these potential risks in the informed consent document.
3. **Data Collection**

Internet-based data collection methods can range from the use of existing data and observations to interventions and survey/ interview procedures.

* 1. ***Existing Data***: Research utilizing data that are both existing and public is not considered human subjects research and does not require HSP review. Data only accessible through special permission are generally not considered public. However, if steps are required to access data (e.g., registration/ login, payment, etc.) but access is not restricted beyond these steps (e.g., anyone who creates a username and password can access the data) the day may qualify as publicly available. ***When determining whether or not data are public, the investigator must decide if there exists an expectation of privacy.*** If the data were not intended for public use, even if the data are technically available to the public, the data should be considered private. Researchers accessing data which contain identifiers and are not publicly available must obtain HSP review and approval.
	2. ***Observations:***  When online research procedures are utilized, the investigator must be sensitive to the definition of public behavior. While one may be navigating in a public space, that individual may have an expectation of privacy, and investigators need to be sensitive to that expectation.
		1. Example: An investigator wishes to collect data from discussions posted in an online community support group for cancer patients. The online community is technically public, in that anyone can view and join in on the discussions, but ***some group participants are there to provide personal experiences and support regarding living with cancer and may believe that all discussions and personally identifiable information will remain private.***

Research in spaces that are not public or that maintain an expectation of privacy must be reviewed at the non-exempt level. In order to make this determination, it is ***important that investigators be familiar with the online space in which they intend to conduct research***.

* 1. ***Chatrooms:*** When navigating in a chatroom, it is important that those present are able to let the researcher know if they are not comfortable with the researcher’s presence and that the researcher respects these wishes. Because access to chatrooms can prove difficult for investigators and chatroom participants are not always eager to have a researcher in their midst, one suggested technique is for the investigators to create their own chatrooms just for research purposes. Investigators can introduce themselves to individuals joining the chatroom with a message informing them about the study and asking them for their informed consent. This is a good method to make sure that all participants are fully aware of the research and have consented to participate.
	2. ***Surveys:***  Survey research is one of the most common forms of internet-based research. Researchers are advised to format survey instruments in a way that will allow participants to refuse to answer specific questions.
		1. Ex.: The list of responses can include an option such as “Decline to answer.”

Additionally, participants must always be given the option to withdraw from a study, even while in the middle of a survey.

Use of Survey Monkey.com, Psychsurveys.org, Mechanical Turk, and other online survey tools is permitted for most minimal risk studies using online survey procedures. Investigators should review confidentiality measures and data security policies for the given online survey tool and make sure that they are described in the protocol. If security measures are not in line with HSP requirements, use of the given survey company may not be approved. Research participants also need to be informed of data security measures.

* 1. ***Interviews:*** Conducting interviews online allows researchers to gather information from respondents who would have been difficult to contact otherwise, such as a very geographically dispersed population. Interviews may be conducted over the internet using email or chat technology such as Google Chat, instant messenger, etc. When conversing with a research participant via online chat, investigators should consider the inability to read visual and auditory cures, which can lead to possible misinterpretation of both questions and responses. Voice intonation and facial expressions are often used to convey meaning. Thus, investigators may need to ask clarifying questions in order to accurately interpret responses, and provide additional information in order to be sure that participants understand the questions. On the other hand, internet-based video chat technology such as Skype or Face Time may be employed for interviews which will allow researcher and participant to interact with more transparency.
	2. ***COPPA:*** Operators of commercial websites and online services directed towards children less than 13 years of age that collect personal information from these minors must comply with the Children’s Online Privacy Protection Act (COPPA). The goal of COPPA is to protect children’s privacy and safety online, recognizing the ease of access that children often have to the web. COPPA requires website operators to post a privacy policy on their website and create a mechanism by which parents can control what information is collected from their children and how such information may be used.

 For more information on COPPA, see: <http://www.ftc.gov/privacyinitiatives/childrens.html>.

* 1. ***Other Considerations***:
		1. When recording material that would otherwise be temporarily posted online, consideration should be given to whether the act of recording this information potentially creates risks for participants. For example, information is, at times, posted on the internet by a third party without the consent of the involved individuals. If a study is likely to record illegal or socially undesirable activity, the investigator should judge whether or not recording this information would create risk for the participants and, if so, reconsider using or retaining the data.
		2. ***TOS:*** Investigators should make sure to review any applicable Terms of Service (TOS). TOS outlines the rules a person or organization must observe in order to use a service. Internet service providers (ISPs) and all websites that store personal data for a user have TOS; in particular, social networking sites, online auctions and financial transaction sites. Some sites and social networking outlets, such as Facebook, may have their own policies regarding ownership and use of data retained on their site. The investigator should be aware of, and if appropriate, disclose this information to participants.
1. **Data Security:**  The investigator must consider additional data-security issues when conducting internet-based research.
	1. ***Researchers must take special care to treat online identities (personas or avatars) and their corresponding character names like real identities. People care about the reputation of their personas and these aliases can usually be traced back to real-world names.***
	2. Though it may not be the intention of the researcher to collect personal identifiable information, internet protocol (IP) addresses can easily be utilized to identify respondents. Proper confidentiality measures need to be in place in order to protect the participants’ identities. These measures include password-protection and encryption.
	3. All identifiable or coded data transmitted over the internet must be encrypted. This helps ensure that any data intercepted during transmission cannot to decoded and that individual responses cannot be traced back to an individual respondent. It is important to note that encryption standards vary from country to country and there are legal restrictions regarding the export of certain encryption software outside U.S. boundaries. It is the investigator’s responsibility to research possible restrictions and revise data security measures accordingly.
	4. The level of security should be appropriate to the level of risk. For most research, standard security measures like encryption and secure socket layer (SSL) are sufficient. However, research involving particularly sensitive topics may require additional protections such as housing data on a professionally managed server.

**Glossary**

**Blog:**  A website used as a journal; can be personal or professional in nature.

**Chatroom:** An online location where individuals can come together to have text-based chat discussions that occur in real time.

**Cloud computing:** Distant storage of data management servers typically owned and operated by a third party (i.e., Google Drive, Dropbox).

**Confidentiality:** Pertains to the treatment of information that an individual has disclosed in a relationship of trust, and with the expectation that it will not be divulged without permission to others in ways that are inconsistent with the understanding of the original disclosure.

**Cookie:** A text file placed on user’s computer by a website or web server. Often used to keep track of individuals as they navigate a site, and more broadly, the web.

**Encryption software:** A piece of software that is used to obfuscate information to all of those who do not have the means to decrypt the information.

**Internet Protocol (IP) address:** A numeric address assigned to every computer that connects to a network, or more commonly, the internet.

**IRC (Internet Relay Chat):** A protocol used for hosting and participating in chatrooms.

**Lurking:** A behavior specific to online communities, wherein an individual remains silent, observes, and does not participate in the community.

**Minimal Risk:**  The probability and magnitude of harm or discomfort anticipated in the research are not greater, in and of themselves, than those ordinarily encountered in daily life.

**Online persona:**  An online character or avatar used by an individual.

**Online survey:** Any tool used to collect responses to survey questions via the internet.

**Privacy:** Control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

**Publicly available:** The general public can obtain the data and they are readily available to anyone (without special permission, application, and/or payment) regardless of occupation, purpose, or affiliation, or is available to anyone who meets the terms of a use agreement.

**Secure website:** A site that conforms to best current security practices, such as use of the Secure HyperText Transfer Protocol (https), application of relevant patches, and sound auditing and certificate management.

**Virtual community:** A group of individuals networked together through association with virtual environment, homepage, or other internet medium (e.g., SecondLife).

**References**

Buchanan, E. Gallant, D., Miller, M. (December, 2010). *Navigating Research Regulations and Research Ethics in the Internet Age.* PRIM&R San Diego Conference.

*Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, with Revisions*. Retrieved from <http://www.hhs.gov/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf>.

*UC Berkeley CPHS Guidelines – Internet-Based Research.* Retriveved from <http://cphs.berkeley.edu/internet_research.pdf>.

*UCLA Guidance on Research Involving the Internet.* Retrieved from <http://ora.research.ucla.edu/OHRPP/Documents/Policy/8/Internet_Research.pdf>.