WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

Research Ethics Board Standard Operating Procedures

Guidelines for Internet-based research

SOP NO:	REB-SOP-IV-12.001	**Revision Date:**	February 13, 2017
CATEGORY	Research Ethics Board	**Reviewed/Effective Date:**	February 13, 2017
SUB-CATEGORY	Section IV: Review of Research	**Original Issue Date:**	February 13, 2017
ISSUED BY:	Research Ethics Office		
APPROVED BY	Vice President, Research		

The WCH REO webpage version of this document is considered the most current.
Please ensure that you have reviewed all linked documents and other reference material within this SOP

1.0 PURPOSE:

The purpose of this Standard Operating Procedure (SOP) is to describe the decisions that the Women's College Hospital (WCH) Research Ethics Board (REB) may make resulting from its review in regards to using internet-based research.

Internet-based research can provide an easy method by which to gain access to a large number of potential participants. Observations, surveys, interventions, and analysis of existing data are commonly used methods of internet-based research. Internet-based research raises a number of challenges concerning human participant protection and the application of federal guidelines and ethical principles.

Topics such as privacy, confidentiality, recruitment, and informed consent become complicated when research is conducted online. The purpose of this SOP is to provide guidance on a variety of challenges relating to internet-based research and to help investigators align their research activities with the TCPS2 (2014).

This SOP is based upon the Guidelines for Internet-Based Research at Ryerson University, and used with permission.

2.0 DEFINITION(S):

See Glossary of Terms

3.0 RESPONSIBILITY:

This SOP applies to the REB Chair, Vice-Chair, REB members, and Research Ethics Office (REO) staff.

The REB Chair, or designee, is responsible for ensuring that a decision is made on social media materials reviewed by the REB.

4.0 PROCEDURES:

4.1. Recruitment

WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

- Recruitment involving email invitations, online advertising, and postings on social media or chat room platforms must be submitted in full for review and approval by the REB before use.
- Investigators must also indicate who will be responsible for posting online recruitment notices, e.g. if using Twitter or Facebook for posting recruitment notices, the investigator must indicate the account from which the tweet or posting will initiate. Best practices would recommend that recruitment notices not be initiated from investigators' personal social media accounts, but rather an account set up primarily for the research.
- Investigators must provide as much detail as possible about where social media postings will be placed, e.g., in closed/open/moderated groups, in paid sites, in other types of groups or pages.
- Recruitment using online advertising platforms must not be placed in "employment" sections or sections for those seeking paid work**.**
- Investigators must be cautious of participants potentially misrepresenting themselves and should take all feasible steps to authenticate participants during the recruitment and/or screening process. Further care should be taken to differentiate human and machine activity and input where necessary, using Captcha technology.
- Providing each study participant with a Personal Identification Number (PIN) to be used for authentication in subsequent computer-and internet-based data collection is considered to be best practice. In this example, the PIN used must not be one that could be used by others to identify the individual (e.g. uniquely identifying number, phone number, birth date, etc.).
- Minors may be screened out by checking for internet monitoring software such as SafeSurf and RSACi rating or using Adult Check systems. This may be necessary if the study presents more than minimal risk to subjects or asks particularly sensitive questions. Investigators may want to increase the validity of their study by screening out minors if their research is focused on adult participants. In studies deemed to involve no greater than minimal risk, the informed consent document may simply ask participants to actively confirm that they are the appropriate age of majority.

4.2. Informed Consent

- Investigators conducting internet based research must follow the TCPS 2 informed consent guidelines and include required elements of informed consent when generating online consent documents.
- The REB generally accepts 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.
- 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

WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

consent. This would constitute unsigned consent and investigators must explicitly note this in their submission for REB review and approval.

- If the REB determines that documented consent is required, the consent form may be mailed or emailed to the participant who can then print and sign the form and return it to investigators via email, postal mail, or fax.
- The process of requesting consent should not disrupt normal online group activity. Researchers need to be particularly sensitive of this when entering online communities and chat rooms 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 in this context, the possibility of deception or incomplete disclosure may need to be addressed in the researcher's protocol application.
- 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.
- 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. For example, when using a third party website to administer surveys, the website might store collected data on backups or server logs beyond the timeframe of the research project. In addition, third party sites may have their own security measures that do not match those of the investigators' (see Additional Considerations below for more information). Participants should be informed of these potential risks in the informed consent document. For example:
    i. "Although every reasonable effort has been taken, confidentiality during actual Internet communication procedures cannot be guaranteed."
    ii. Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties."
    iii. "Data may exist on backups or server logs beyond the timeframe of this research project."

WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

Research Ethics Board Standard Operating Procedures

Guidelines for Internet-based research

4.3. Data Collection

4.3.1. Existing Data

- Research utilizing data that are both existing and public is not considered human participant research and does not require REB review (TCPS 2, Article 2.2).
- 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 data may qualify as publicly available. The investigator should consult with the REB if they are unsure if the research requires REB review and approval prior to the outset of research activity.
- When determining whether or not data are public, the investigator must determine if there exists an expectation of privacy. The investigator should consult with the REB if they are unsure if the data are public and whether or not the project requires REB review and approval prior to the outset of research activity.

4.3.2. Observations

- Article 2.2 of the TCPS2 notes that "Research that relies exclusively on publicly available information does not require REB review when: (a) the information is legally accessible to the public and appropriately protected by law; OR (b) the information is publicly accessible and there is no reasonable expectation of privacy."
- When online research procedures are employed, the investigator must be sensitive to the definition of public behaviour.
- Despite navigating in a public space, an individual may have an expectation of privacy, and investigators need to be sensitive to that expectation. Consider the example of an investigator who wishes to collect data from discussions posted in an online community support group for illegal substance use. While the online community is public, in that anyone can view the discussions and join the group, group participants may be disclosing personal or sensitive information about their substance use that they may not wish to be shared outside of such a group.
- Research in spaces that are not public or that maintain an expectation of privacy must be reviewed by the REB. In order to make this determination, investigators must be familiar with the online space in which they intend to conduct research. Not only do investigators need to have an insider's viewpoint in order to know whether or not participants have an expectation of privacy, but investigators will often be met with hostility if they are not sensitive to the online community's expectations. Participants of an online community may see the presence of a researcher as

WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

intrusive and clear steps must be taken by investigators to avoid this potential situation as much as possible.

- If an investigator has prior experience in an online community and is already known to its participants, the researcher may have a better chance of being welcomed into the space.

4.3.3. Chat rooms

- When navigating in a chat room, 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 chat rooms can prove difficult for investigators and chat room participants are not always eager to have a researcher in their midst, one suggested technique is for investigators to create their own chat rooms just for research purposes. Investigators can greet individuals joining the chat room with a message informing them about the study and asking them for their informed consent. This is considered to be best practice to be sure that all participants are fully aware of the research and have provided informed consent to participate.

4.3.4. Online Surveys

- Survey research is one of the most common forms of internet-based research.
- Online surveys must be preceded by a consent preamble with an active indication (click here to indicate agreement to take part) of consent built in.
- The elements of consent that are required in any kind of research should be addressed, as relevant, in an online survey consent preamble.
- Best practices can also include multiple choice questions regarding the important elements of consent to assess understanding.
- Researchers are advised to format survey instruments in a way that will allow participants to refuse to answer specific questions and still complete the survey.

Questions can also include, in the list of responses, an option such as, "Decline to answer."

- Participants must always be given the option to withdraw from a study, even while in the middle of a survey and should be provided with clear instructions on how to withdraw and ensure no data are submitted.
- Use of SurveyMonkey.com, Psychsurveys.org, Mechanical Turk, and other online survey tools is permitted for most minimal risk studies employing online survey procedures. Investigators should review confidentiality measures and data security policies for the given online survey tool and make sure that they are well described, using lay terms, in the protocol and the consent preamble.

- If security measures of the online survey tool is not supported by WCH IT, use of the given survey company may not be approved.

4.3.5. Interviews

- Conducting interviews online allows researchers to gather information from participants who would have been difficult to contact otherwise, such as a very geographically dispersed population or individuals who are isolated or located far from the investigator's location. Interviews may be conducted over the internet using email or chat technology such as Google Chat, AOL instant messenger, Yahoo! messenger, etc.
- A complete consent form should be provided to the participant prior to the online interview. While the original signature of the participant may not be realistic nor feasible to obtain, the online interview should begin with a consent process, involving a review of the information in the consent form, an opportunity for participants to ask questions and an explicit confirmation of consent.
- Care should be taken to ensure privacy and confidentiality when using online technology to conduct interviews, e.g. participants and researchers should each be in a private space that ensures aural and visual privacy.
- Best practices recommend that investigators may need to provide clarifying information, or documents (such as an interview guide) to participants ahead of the interview.

4.3.6. Additional Considerations

- 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 subjects and, if so, reconsider using or retaining the data.
- 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.

4.3.7. Data Security

- Researchers must take special care to treat online identities (personas or avatars) and their corresponding character names with the same care as real names.
- Even when it is not the intention of the researcher to collect identifiable information, internet protocol (IP) addresses can easily be used to identify respondents. Proper confidentiality

WOMEN'S COLLEGE RESEARCH INSTITUTE
Health care for women | REVOLUTIONIZED

Research Ethics Board Standard Operating Procedures

Guidelines for Internet-based research

measures need to be in place in order to protect the subjects' identity. These measures include password-protection and encryption of all collected data.

- All identifiable or coded data transmitted over the internet must be encrypted. 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 Canadian boundaries. It is the investigator's responsibility to research possible restrictions and revise data security measures accordingly.
- The level of security should be appropriate to the risk. For most research, standard security measures like encryption will suffice. However, research involving particularly sensitive topics may require additional protections such as housing data on a professionally managed server.
- For any electronic data being transported between locations, the protocol must outline, in detail, how data are being secured and protected during transport.

5.0 REFERENCES:

1. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans 2014 (TCPS2)
2. Ryerson University Research Ethics Board (REB) Researcher guidelines. http://www.ryerson.ca/research/services/ethics/human.html
3. The International Conference on Harmonization Good Clinical Practices (GCP Guidelines as adopted by Health Canada, Section 3.0
4. US Department of Health and Human Services (HHS) Title 45 CFR 46.109, 46.111
5. US Food and Drug Administration (FDA) Code of Federal Regulations (CFR), Title 21 CFR 50 and 56
6. Sunnybrook Health Sciences Centre Research Ethics Board Standard Operating Procedure– *Research Ethics Board Review Determinations* (REB-SOP-IV-01.003)