APPENDIX N

# RESEARCH INVOLVING THE INTERNET

This form should be completed for studies that collect data via the internet. This may involve internet-based surveys (i.e., Qualtrics), data collection from social networking sites, or monitoring a subject’s internet activity.

Do not use this form if you are only planning to use the internet to transmit case report files (CRFs) electronically between sites or investigators, store data over the internet, or to communicate with participants via email.

Please make sure that the information provided on this form is consistent with the information included on [Human Subject Application – Part 1](https://www.du.edu/orsp/media/documents/new_irb_forms/irb_part_one.docx) and any consent forms.

## Section 1. Use of the Internet

1.1.How is the internet being used in this research? Please provide a general description.

Click here to enter text.

1.2. Will you be observing internet activity (e.g., chatrooms, social media, web browsing)?

[ ]  Yes

[ ]  No

 If Yes, describe the setting and nature of the online activity being observed:

 Click here to enter text.

If Yes, does the privacy policy for the site where you will be observing activity include reference to research or other information relevant to your research? Please explain.

Click here to enter text.

Will subjects be aware that their activity if being observed (consider chat room access, privacy setting on social media sites, privacy warnings on web pages, etc.)

[ ]  Yes

[ ]  No

1.3. Will you be collecting data over the internet (e.g., survey tools)?

 What website or survey tool will you be using?

 [ ]  Qualtrics

[ ]  MTurk

[ ]  Other (please specify) Click here to enter text.

1.4. Informed Consent

Does the software provide a record that captures that a respondent has consented to the survey before survey initiation?

[ ]  Yes

[ ]  No

 If ‘YES’, please describe the implied consent and attach it within the IRBNet package submission.

 Click here to enter text.

1.5. Secure Transmission

Information sent to and from web sites can either be transmitted in clear text that could be read if the information was intercepted by a third party (http protocol) or encrypted so that a third party could not read the intercepted information (https protocol).

Are there controls in place to prevent a respondent from accidentally entering survey data via the http protocol instead of the https protocol (i.e., does the server display an error message or automatically re-route the respondent to an https page)?

[ ]  Yes

[ ]  No

Does the survey tool use https encryption?

[ ]  Yes

[ ]  No

1.6. Database Security

Do researchers have access to their data in the database via a username and password?

[ ]  Yes

[ ]  No

Has the software company maintaining the database signed confidentiality agreements preventing them from improperly accessing or disclosing information contained in those databases?

[ ]  Yes

[ ]  No

1.7. Server Security

Are the servers containing research data located in the data center, with physical security controls and environmental controls?

[ ]  Yes

[ ]  No

1.8. Back-ups

Are the data backed up nightly?

[ ]  Yes

[ ]  No

Is there a finite period of time in which a deleted dataset can still be retrieved? (It is recommended that the investigator inquire about the length of that period.)

[ ]  Yes

[ ]  No

1.9. IP Addresses

Is the respondent’s IP address masked for the researcher?

[ ]  Yes

[ ]  No