10 West Madison Street #11
Baltimore, MD 21201

Complete Wellness INSTITUTE

Phone: (443) 438-7863
Fax: (443) 957-9485

INTERNET RESEARCH POLICY

I. RECRUITMENT

The text of the recruitment script, and the context in which the recruitment takes place (e.g. posting a message on a newsgroup, mass emailing, and websites created for recruitment of participants) must be reviewed and approved by the Complete Wellness IRB.

In order to authenticate respondents, investigators shall provide 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.

II. DATA COLLECTION

Any identifiable data collected from human participants over computer networks must be transmitted in encrypted format.

III. DATA ADMINISTRATION

A. Using a Server

If a server is used, the server must be administered by a professionally trained person with expertise in computer and internet security.

Access to the server must be limited to key project personnel.

The server must be subject to the periodic vulnerability assessments to determine that the server is patched according to industry best practices.

B. Using the Cloud

If research data is stored in the cloud, a Business Associate Agreement must be obtained from the vendor maintaining the cloud-based system.

If data are stored in the cloud (i.e., at multiple, dispersed sites) additional considerations, including data privacy laws at the local storage site(s) and regulations other than those at the research site, may apply. These include, for example, the European Data Privacy Directive 95/46EC or the Canadian Privacy Act and the Personal Information Protection and Electronic Documents Act. Agreements with data storage and processing entities should acknowledge the investigator's and any business associates' responsibilities to comply with relevant requirements, and subjects should be informed of such arrangements as appropriate.

IV. DATA STORAGE AND DISPOSAL

If a server is used for data storage, personal identifying information must be kept separate from the data, and data must be stored in encrypted format.

It is recommended that competent data destruction services be used to ensure that no data can be recovered from obsolete electronic media.

V. ONLINE INFORMED CONSENT FOR SURVEY-BASED RESEARCH

If you are distributing surveys through email, you should include the following statement in your consent process:

> *Although it is unlikely that anyone will try to gain access to your email, you have the right to know that email transmissions are not private and therefore transmission of information through this form cannot be guaranteed to remain confidential."*

The consent line should say, "*By completing the survey you are agreeing to participate in the research*" and include "*I agree*" or "*I do not agree*" buttons.

The following statement is required to be listed on the consent form:

> *Confidentiality will be maintained to the degree permitted by the technology used. Your participation in this online survey involves risks similar to a person's everyday use of the Internet*.

The consent must disclose that if a participant completes an anonymous survey and then submits it to the researcher, that the researcher will be unable to extract anonymous data from the database should the participant wish it withdrawn.

If the Complete Wellness IRB approves internet research which requires documented consent, and does not maintain the anonymity of participants, the researcher may email the consent form to participants who may then type their name and the date into the spaces provided on the consent form, and returns it to the researcher via email, if the Complete Wellness IRB determines that documented consent is required. Some survey programs allow a similar consent process to be built into the survey itself, which can also be permitted by the IRB.

VI. REVISION HISTORY

Date	Description of Revisions
5/20/2021	Initial document

10 West Madison Street #11
Baltimore, MD 21201

Complete Wellness INSTITUTE

Phone: (443) 438-7863
Fax: (443) 957-9485

SURVEY SOFTWARE CHECKLIST

- ❑ The software must provide a record to the researcher that captures that a respondent has consented to the survey before the survey.
- ❑ Record of consent must be logged with a timestamp.
- ❑ The survey must use https encryption.
- ❑ Controls to prevent a respondent from accidentally entering survey data via the http protocol instead of the https protocol are highly recommended.
- ❑ Researchers should have access to their data in the database via a username and password.
- ❑ The software company maintaining the research database must have signed confidentiality agreements preventing them from improperly accessing or disclosing the information contained in those databases.
- ❑ The servers that contain the research data should be located in a data center with physical security controls and environmental controls.
- ❑ Data should be backed up nightly.
- ❑ A finite time period in which a deleted dataset can still be retrieved is strongly recommended.
- ❑ The respondent's IP address must be masked from the researcher.