# Guidance: Data Collection via Web-Based Surveys

In research, collection of data via web-based surveys is common. Numerous third parties offer platforms on which one can create, deploy, collect and analyze surveys using a web-based interface. While Marywood University (MU) allows the use of online surveys for a majority of human research, several factors need to be considered when designing studies. This guidance document addresses these factors.

## Anonymity or Confidentiality – One, Not Both


Investigators often confuse the terms anonymity and confidentiality. In human research, both are to be considered form the point of view of the investigator. **Anonymity** exists if you not only collect data without any personal identifiers, but also cannot associate identities with the information, such as through a code or a process of deduction (e.g. many demographics with a small sample size). **Confidentiality** exists when data contain identifiers or you may associate identities, but you manage the information in such a way as to protect the privacy of the individuals from outside parties. When communicating with your participants in advertising or the informed consent process, be sure to use the appropriate term.

## Survey Platforms

**Email** is allowed for *recruitment* (advertising), but is not acceptable for the *collection* of returned survey responses. It is not always secure, and email addresses may identify a specific set of responses. Please use one of the below platforms to collect data instead.

**Qualtrics** | Qualtrics Basecamp | Survey Overview | Anonymous Link | Anonymous Responses
The official survey platform of MU, Qualtrics is free to all MU students, faculty and staff. It offers practical drag-and-drop functionality for designing surveys, complex branching logic, and the ability to collaborate on surveys, along with instructor oversight. It uses the TLS method of encryption (HTTPS) and survey security options for transmitted data, such as password protection and HTTP reference checking. It is also HIPAA compliant with a Business Associate Agreement. MU's Educational Technology staff provides support of the platform. To create an account and be automatically added to Marywood University's license, log in at https://marywood.co1.qualtrics.com/login with your Marywood username and password.

**REDCap - Research Electronic Data Capture** | Brief Overview | Index of Training Videos
Part of REDCap's consortium, MU allows use of this free, secure application for many web-based surveys and databases. However, MU's Educational Technology staff does not provide user support for the product other than account set up. To request an account, contact the Help Desk at helpdesk@marywood.edu or 570-340-6070. REDCap offers tutorial videos, linked above (scroll past log in).

**SurveyMonkey®** | Making Responses Anonymous | Survey Monkey's IRB Guidelines
Offering SSL encryption, Survey Monkey is reasonably secure with an appropriate account plan. However, MU's library account is prohibited for use with human subjects. Therefore, personal accounts must be purchased, and MU's Educational Technology staff does not provide user support. Specify in

your research application the type of account you will use (personal, advisor's, and account level). We highly recommend that you use Qualtrics instead.

**SONA Systems** | SONA Psychology Department Sign In
Used by MU's Psychology Department for its participant pool only, SONA allows study recruitment and scheduling, but also survey administration. The platform may *host* surveys or *link* to third-party platforms (e.g. Qualtrics). SONA states that it is HIPAA compliant with a Business Associate Agreement and also Common Rule compliant. The Psychology Department provides user support. If using SONA, be sure to describe exactly *where* the survey will be hosted – within SONA itself or on another platform.

**Question Pro**
Because SSL encryption is only available with top-tier, paid accounts, MU allows Question Pro on a case-by-case basis for minimal risk research. MU's Ed Technology staff does not provide user support. We highly recommend that you use Qualtrics instead.

## Survey Settings and Security

In order to best protect human research subjects, you must familiarize yourself with your chosen survey platform's features. Describe the platform and all appropriate settings in your IRB/ERC application.

- An Internet Protocol (IP) address is a unique, potentially identifying number assigned to every networked device. Because your survey platform might collect it by default, explain that you will disable the feature if not necessary for your research. The board may request that it be disabled.
- Know the platform's security levels and settings to protect data during transmission. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are standard security technologies for encryption between a web server and a browser. You will see them in a URL as "https://."
- Consider and describe whether you will create one, general survey link to send to all subjects from your personal email account, whether someone will forward a message for you, or if you will email subjects directly through the survey platform itself, where individual survey links will be created and traceable.
- Consider the ability to skip questions or provision of "prefer not to answer" responses. Paper surveys make this possible, but survey sites do not unless you configure responses in this manner.
- If offering compensation (e.g., payment, raffle entry for a prize), consider how and whether the method will identify anyone. For instance, will you keep raffle entries separate from subjects' survey responses? Does the site offer a feature to assist with this or will you have participants email you separately to enter? Will you create a second survey for the entry, so that the entry will not link to the results? Will you attempt to identify anyone through a time/date stamp with the main survey's time-stamped results? Will you send the winner a digital code or physical gift card, which would require an identifiable address?

## Survey Informed Consent Elements

Since web-based surveys differ from traditional, paper-based surveys, informed consent must be adjusted to fit the method.

- Plan for your informed consent form to appear as the first screen after your subjects click an emailed web link, scan a QR code, etc. Submit your consent form in IRBNet *as its own document* (DOC format), so that any requested modifications may be tracked. Once approved, you'll insert the informed consent form as the survey's first page at the site.
- While you need to use a secure platform and protect responses, you cannot absolutely control third-party access during transmission. Therefore, add the required statement concerning Internet procedures to the confidentiality section of the informed consent form. The language may be found in the template's instructions (in table and labeled as "Internet or Web-based transmissions").
- Federal regulations mandate the option for subjects to withdraw at any time, even after their activities have ended. With anonymity, however, it is not possible for subjects to withdraw later, because you won't be able to identify specific responses. Therefore, under the Taking Part is Voluntary section, explain that withdrawal may happen at any time, but only until they submit, and explain how (e.g. "You may withdraw at any time before you submit. To do so, close your browser."). Also mention what will happen to their responses up to that point (used or discarded).
- Adjust the statement at the informed consent form's end about being "*given* a copy" to "may *save* or *print* a copy," unless there's some reason why they are receiving a hard copy.
- After the Statement of Consent, include some sort of "I agree/I disagree" or "Next" buttons so that subjects may advance to or exit the survey.

## IRB: Documentation of Informed Consent or Waiver of Its Documentation

**Documentation of informed consent** refers to use of a **written informed consent form,** approved by the IRB, which will be **signed**, including in an electronic format, by the subject or the subject's legally authorized representative. Unless waived, **documentation is required** for all IRB-reviewed research (expedited or full). **Documentation is not required** for exempted studies, unless a specific law applies (e.g. FERPA). No signature lines appear on the ERC Informed Consent Template for this reason.


For full or expedited studies, IRB waivers of documentation may be granted if they meet one of three, Federal criteria for such waivers. If you wish to waive documentation, you must complete and submit a *Waiver of Documentation of Informed Consent Request Form*. A waiver of documentation only waives the signature, not the overall consent process or form.

The Common Rule at 45 CFR 46 does not explicitly define "electronic format." However, it is important to note that **simply proceeding from an electronic informed consent form to a survey is not an electronic "signature"** per se. It is an agreement to participate, but is not considered *documentation*.

If waiver of documentation cannot be granted, you will need to propose the collection of signatures offline, or enable actual e-signatures through a specific survey platform setting, such as through use of a mouse, stylus or finger, or use of a pre-scanned "wet signature." These settings are available in some of the platforms described above. There may be other systems which identify and authenticate a particular person as the source of the e-signature and consent (e.g. University single sign-in portals), which may be acceptable as documentation. You will need to describe all procedures in your IRB/ERC application and enable platform settings, if approved.

Keyboard Photo by Sergi Kabrera on Unsplash