# Institutional Review Board (IRB) Application Tips

## Introduction

Institutional Review Boards, or IRBs, are institutional committees that oversee research involving human subjects in a given institution, such as Human Subjects Review Boards, Committees for Protecting Human Subjects, etc.

IRBs exist for two important reasons:

1. To safeguard the rights and well-being of individuals participating in research studies
2. To balance potential risks to participants with potential benefits to society

Typically, one or two members of an IRB will review each research proposal, depending on the characteristics of the proposal research and the IRB's review procedures. Although the process of IRB review can seem time-consuming for researchers, these peer-review processes help maintain the integrity of the social sciences and ensure the safety of participants as a whole.

PsychData was designed to satisfy the standards of social science IRBs for online data collection and is continuously evolving to meet these standards, particularly in the field of psychological research.

## IRBs and Web Based Research

Web-based psychological research is a relatively recent development, and IRBs are still developing policies and procedures to manage these new tools. As a researcher, it is important to help inform IRB members about online research. We provide the following information to assist you in informing your research application as it relates to your IRB about online research. The information provided below has addressed nearly all of the issues reported by our users regarding IRB approval for web-based research.

### Informed Consent

IRBs require participants to provide informed consent before taking part in survey research. Consent for web-based surveys can be obtained through various methods. The most popular approach is to ask participants to perform a specific action to express their consent to participate in the survey. When using PsychData, there are several ways you can do this:

1. Require your participants to click on a button to indicate their consent to participate.
    - Use our Survey Designer to enter your Informed Consent text. At the end of your Informed Consent text, include a statement similar to this: "If you have read and understand the above statements, please click the 'Continue' button below to indicate your consent to participate in this study."
    - Insert a Page Break. This will result in an Informed Consent Page that is separate from the rest of your study. Thus, by performing the specific action of clicking on the "Continue" button your participants clearly indicate their informed consent prior to viewing or completing any questions in your study.

2. Require your participants to provide a specific piece of information, such as a valid email address. Simply insert a required question immediately after your informed consent text and prior to your page break.
3. Require your participants to provide a digital signature.
4. If your IRB requires a physical signature, then we recommend the following: Immediately after your informed consent statement enter as many questions as are required of you. Enter your instructions to the participant (e.g., please enter your information, print this page using the link below, sign on the line below, and mail to the following address). Next, enter the unique Respondent ID field into your survey followed by text that says, "I, _____, consent to participate in this survey." The participant will enter their information, print out the page, sign it, and mail it to you. Because you can include the Respondent ID in your dataset, you will be able to track who sent in the form and who did not.
5. Waiver of Documentation - If you will not be asking for a signed paper, some IRB's may require a waiver of documentation (i.e., signature) of informed consent from your IRB. This is NOT a waiver of consent, but rather a waiver of obtaining a signature on the consent form and exact procedures will vary by IRB.

## Survey Completion Risks

Risks during the actual completion of survey questions are only slightly different with PsychData than with traditional methods.

1. Participants are likely to have more privacy at their computer than in a lecture hall or classroom.
2. PsychData has addressed concerns about potential third-party access to survey data by placing all surveys in our unique Secure Survey Environment (SSE).
    - Survey pages are designed to prevent users from viewing completed surveys by using the "Back" button, reducing the chance of accessing previously entered data.
    - Our survey platform has extra security features to make sure that a participant's responses can't be retrieved from their computer. First, all survey pages are dynamic and generated from a database, rather than being static web pages that could be saved on the participant's computer. Second, we use redundant server-side code to ensure that surveys always load directly from our server and not from a previously saved version. Finally, after completing the survey, the participant is encouraged to close the browser window.

## Data Security During Transmission

All surveys hosted with PsychData are encrypted using 256-bit SSL Technology (Secure Socket Layer), the industry standard for safely transmitting credit card information over the Internet. This technology encrypts BOTH the questions displayed to participants and their responses. Thus, all responses are encrypted from creation until they reach the PsychData database.

It's HIGHLY unlikely for anyone to intercept the data while it's being sent from the internet browser (examples include Internet Explorer, Firefox, Safari, Chrome) to the PsychData database, considering the motivations of someone trying to get research data over the internet versus papers stored in an office or credit card information.

However, if encrypted data is intercepted, it cannot be decoded without the unique encryption key held only by PsychData.

## Safety of Stored Data

Once your research data is stored on a PsychData server, it is kept in a separate database that only researchers with the correct username and password can access. PsychData employees do not examine a client's data unless asked to do so by the client. All of our researchers are trained in research ethics concerning human subjects.

## Control of Stored Data

As a researcher, you have full control over your data, including the ability to delete all your data once your survey is complete.

All data stored at PsychData is backed up daily and kept in a highly secure facility. The data is usually overwritten after seven days. This means that once you delete your data, it will be permanently removed from our backups in about one week.

## Identifying Information

To conduct their research, many researchers need to gather information that identifies their participants. It's essential that this information is handled separately from the research data, as per IRB guidelines.

PsychData manages identifiable information by allowing you to connect two surveys. This allows you to collect, store, and access participant information and research data separately. If you need to gather identifying information while also collecting anonymous research data, this method is the safest choice.

## IP Addresses

An IP address is a unique number used to identify computers on the Internet. It can be static (always the same) or dynamic (changes with each connection). Sometimes, IP addresses can change multiple times during the same connection. They usually represent either an institution, like a university or company, or an Internet Service Provider, like AOL.

1. Researchers at PsychData can choose whether or not to include the IP address of each participant in a survey or surveys.
2. Some researchers use IP addresses in conjunction with date and time stamps to filter out duplicate entries and understand the geographic distribution of participants. PsychData can automatically collect IP addresses for these purposes.
   However, IP addresses can indirectly identify participants, although, rarely does an IP address belong to an individual user.
   PsychData also allows excluding IP addresses from data collection to protect confidentiality. Keep in mind that while IP addresses pose a potential risk to confidentiality, they are less concerning than other identifiable information such as handwriting, fingerprints, postal addresses, or email addresses. IP addresses should be considered in the appropriate context.
3. All commercial websites, and many others, routinely analyze the IP addresses of site visitors, such as participants, customers, and web surfers. PsychData is no exception. However,

PsychData only examines this data in aggregate and will never sell, disclose, or share this information.

## Unique Respondent ID Number

At PsychData, everyone who completes a survey receives a unique number called the Respondent ID Number. Researchers can use this number to create a confirmation page for participants within or at the completion of the survey. The researchers can also choose whether or not to download or exclude this data. This feature is important because it gives participants an identifier that represents their survey participation without revealing their identity.

Based on our experience, this information has addressed a majority of the concerns that IRBs have about online data collection. Because of our dedication to ensuring security, confidentiality, and privacy in web-based social science research, many IRBs approve of research conducted with PsychData online. We invite you to reach out with any questions, concerns, suggestions, or feedback at support@psychdata.com.