IRB SECURITY REVIEW GUIDANCE, ONETRUST

The Office of Information Security (OIS) supports our community's important work of administration, academia, and patient care by evaluating tools and services from an information security perspective. Our purpose is always to protect privacy and secure the work of our trailblazing knowledge seekers. The software platform, OneTrust, makes it easier for the OIS to work with users to identify, track, and mitigate security risks involved in the diverse projects underway at our institution.

In the IRB Security Review process, our team works with research coordinators to evaluate security risks involved in the research process. With a particular eye toward securing personally identifiable information (PII) and protected health information (PHI), we'll assess the suitability of selected tools and services, as well as the security of proposed data flows. This process empowers our researchers to make better security decisions for protecting the privacy of their participants and securing data throughout the research process.

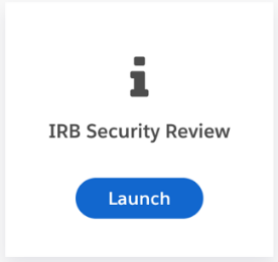
To begin and IRB Security Review, users need to complete a form in OneTrust.

Please Note

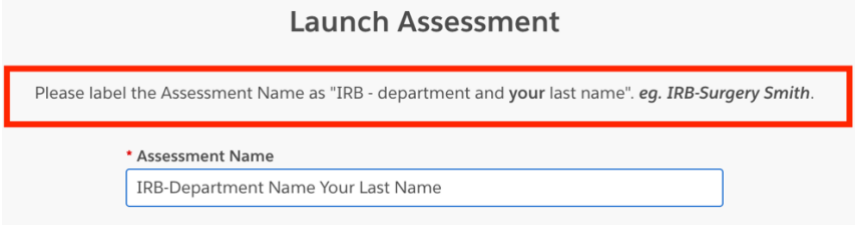
- Please be prepared to upload a copy of the proposed data flow, the research protocol, and consent/assent forms.
- Please be aware that all questions except for question 1.6 are required.

Creating a New Form

1. From the Forms page on the OIS website, click "IRB Security Review."
2. Enter your WUSTL email address in the OneTrust login page. If you aren't already logged in with DUO, you will be prompted to complete our WashU 2FA process.
3. From the Self-Service Assessment main page, click "Launch" under IRB Security Review.



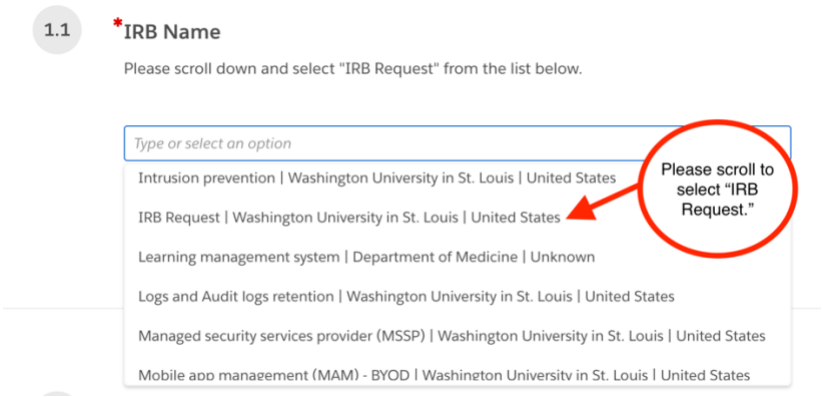
4. Enter a name for your Assessment. Please use the following format "IRB-department name your last name."



5. In the sidebar to the left, please click on the questions for IRB review.

Form Questions

1.1 IRB Name
Click and scroll to “IRB request”



1.2 Select the button for IRB Review.

1.3 Contact name for the project.

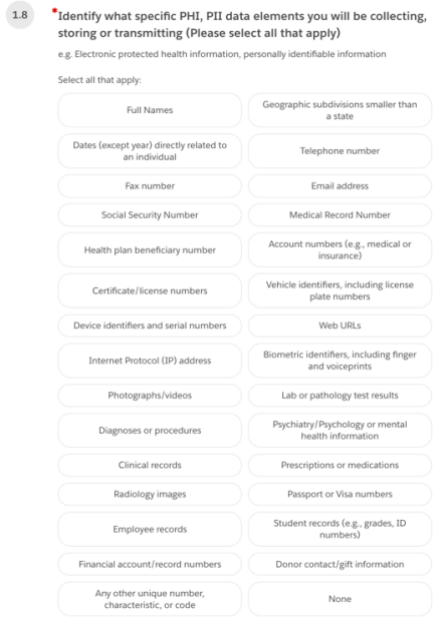
1.4 Contact email address.

1.5 Name of study project

1.6 Name of HRPO representative

1.7 Prove a short summary of the purpose of the technology and how it pertains to the study. *Why did HRPO route you to the Office of Information Security? Please do not copy directly out of your protocol.*

1.8 Identify what specific PHI, PII data elements you will be collecting, storing, or transmitting.



1.9 From the same list, identify what specific PHI will be shared with the vendor or sponsor.

1.10 Describe how the PHI data will be transmitted.

1.11 Identify where the PHI or PII will be created, stored, or transmitted. For example, network share, workstation, USB drive, or external sites. Please provide product and vendor names.

1.12 Please attach a data flow chart illustrating how the data will move to and from the vendor and where the data will rest. An attachment is required.

1.13 If you are using a vendor, please indicate where WashU has a Business Associate's Agreement (BAA) with the vendor. Please select "yes" or "no." For more information about BAAs, please visit The HIPAA Privacy Office BAA page Business Associate Agreement (BAA) | HIPAA Privacy Office | Washington University in St. Louis

1.14 Will there be any affiliated hospital systems (BJC) devices, data, equipment, or workforce members involved in this project? Please select "yes" or "no."

1.15 If you answered "yes" to 1.14, please explain what affiliated hospital system (BJC) devices will be use. Please type your response in the text box.

1.16 Have you consulted with our affiliated hospital system (BJC) on the study? Please select "yes" or "no."

1.17 How is the PHI/PII protected. For example, in a password-protected document, on an encrypted USB device, secure transmission, etc. Please type your response in the text box.

1.18 Is the data you are capturing de-identified? Please note that if you are using PHI and/or PII, then it is an "identified dataset." Please select "yes" or "no."

1.19 If you selected "yes" to 1.18, please describe the process you're using to de-identify the data. Is the process manual or automated? Please type your response in the text box.

1.20 If you answered yes to question 1.18, please respond to question 1.20: How do you verify/test the output of a report is de-identified after a change (such as added fields to a form), and that it is not exposing PHI/PII? Please type your response in the text box.

1.21 Will the research information be stored on a WashU supported device? Please select "yes" or "no."

1.22 Are you using social media for outreach? Please select "yes" or "no."

1.23 If you answered "yes" to question 1.22, please respond to question 1.23: If so, how do you address social media outreach in your Informed Consent? Please type your response in the text box.

1.24 Identify the sponsor for this study. Please type your response in the text box.

1.25 Is this a multi-center study. Please select "yes" or "no."

1.26 If you selected "yes" to question 1.25, please answer question 1.26: Is Dash you the coordination location for the data? Please select "yes" or "no."

1.27 If you answered "yes" to question 1.25, please answer question 1.27: What type of data will be hosted by the data coordinating site? For example, identifiable, limited data set, de-identified data, etc. Please type your response in the text box.

1.28 Will a survey be used in the study?

1.29 If you answered "yes" to question 1.28, please respond to question 1.29: Who will host the survey and where will the data be stored? Is the survey host controlling that data, or do we store it at WashU? Please type your response in the text box.

1.30 If you answered “yes” to question 1.28, please answer question 1.29: Please provide a copy of the survey. Please upload the survey as an attachment.

1.31 Will the study capture audio and/or video recordings? Please select “yes” or “no.”

1.32-1.37 If you responded “yes” to question 1.31, please answer questions 1.32-1.37.

1.32 Choose the recording options. Select “audio,” “video,” or “both.”

1.33 Please describe how the session/interview will be recorded. Please type your response in the text box.

1.34 How will the device use to record the session/interview be secured (physical and technology)? Please type your response in the text box.

1.35 Where will the recording be stored? Please type your response in the text box.

1.36 How will the recording be transmitted? Will it be transmitted over the internet, by SMS, or some other means? Please type your response in the text box.

1.37 How will the recording be secured? Please type your response in the text box.

1.38 Will you be using transcription services? Please select “yes” or “no.”

1.39 If you answered “yes” to 1.38, please answer 1.39: What transcription service were you planning to use? Please type your response in the text box.

1.40 Please submit protocol, consent/assent, and any other supporting documents with Security Review Submittal. Please attach everything that is deemed important to the project.

Once you have answered all required questions, the blue “Submit” button will become available. Click it to submit your form or click “Save and Exit” to come back later.