Data Safety Submission Guide

Data Safety and Security System

December 8, 2023

Table of Contents

Logging In

The Data Safety system is secure, which means only authorized individuals have access to it. When you log in to the system, you get a personalized view of the information and possible actions pertinent to you.

To log in:

1. Locate your HarvardKey and password
2. Navigate to researchsafety.harvard.edu
3. Ensure the correct login type tab is selected
4. Enter your credentials (HarvardKey and password) in the appropriate spaces
5. Click the "Login" button
6. Once authenticated, you will be taken into the Data Safety system, to your personal workspace.

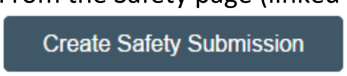
If you are unable to log in, contact the Research Safety Help Desk at rshelp@harvard.edu.

Creating a New Protocol

In the data safety system, a new protocol is a new submission on which the plans for management of one or more sets of data can be proposed for review by the appropriate security reviewer at the University. You can create a new protocol for data safety review by entering information into a series of online forms. The forms tell you where to attach files to provide supporting information. The forms may contain required information, identified by a red asterisk (*). You cannot proceed without providing that information.

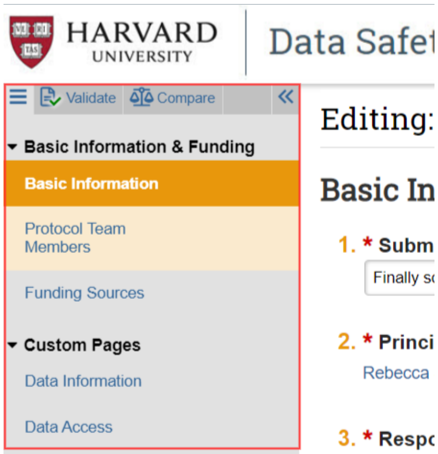
The simplest approach is to follow the forms in order, answering the questions and clicking Continue to save your information and move to the next form. When you reach the end of the series of forms, click the Save & Exit button to return to the protocol workspace.

To create a new submission for review:

1. From the Safety page (linked in the top menu), click **Create Safety Submission**.


2. Fill in the applicable boxes, answer the questions, and attach appropriate documents.
3. Click **Continue** to move to the next form.


4. Use the navigation menu on the left-hand side of the page to go to a specific section. You can collapse this menu by clicking the ≪ button, or if it is collapsed, click ≫ to expand it.



5. To save or exit the SmartForm at any time, click on "Save" and "Exit" button in the lower right of the page. Exit will take you to that submission's workspace.

6. When you reach the final page, click **Save & Exit** to exit the protocol.

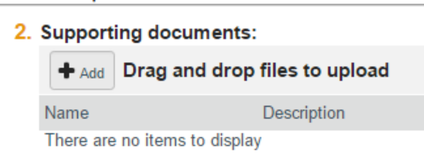
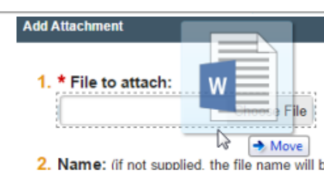
You can continue to edit the protocol until you submit it for review. See Editing a Submission.

Important! The submission has not yet been submitted for review. For instructions, see Submitting Materials for Review.

Tips:

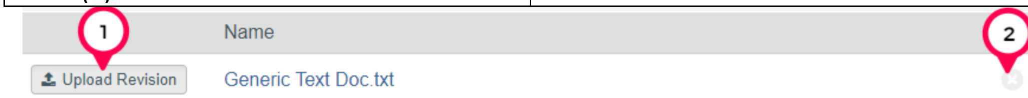
- If a protocol team member plans to create a new protocol which is similar to an existing protocol, the PI on the existing protocol can use the **Copy Submission** activity to create a partially completed form to update and further edit prior to submission.

- Documents can be added to the SmartForm by dragging and dropping them from a location on your computer. There are two different ways to do this, depending on the prompt provided on the form.

Drag and Drop Document Sets	Drag and Drop Single Attachments
Mouse-over to identify if documents can be added from the main page. This does not work in every attachment space.	Drag in single attachments after clicking the "add" button.
	
Reminder: Always name document files wisely (such as with the study number and the document type in the name). The suggested best practice for file names: *StudyNumber_DocumentName_VersionNumber*	

- Items can be updated or removed in the following ways:

Update	Remove
Update items by clicking on the **Upload Revision** button on the left side of the item (1).	Remove items by clicking the X on the far right of the entry (2).



- A continuing review or amendment can be handled similarly to a protocol. For differences, see [Creating a Follow-On Submission after Protocol Approval].

What to Include in a Protocol SmartForm

The SmartForm is a series of web forms where you can input specific information about a protocol. The following section describes what information should go into each space of the SmartForm.

Note: Before visiting the form, it is helpful to review guidance about research data management, including the development of a Data Management Plan at: https://researchdatamanagement.harvard.edu/

SmartForm Section: Basic Information

1. ***Submission title.** Give your protocol a brief, easily identifiable title. This title will identify your protocol throughout the system, such as in your inbox and in the reviewer's list of submissions to review.
2. ***Principal investigator.** The Principal Investigator (PI) is the primary person responsible for the data and for actions in the system. The options PI are limited to individuals with a Harvard ID/HarvardKey.
3. **Primary contact.** The Primary Contact will receive a copy of all communications from the Safety System about this submission, in addition to the PI. This person cannot edit or comment on the record.
4. ***Responsible department.** Indicate the PI's department. This will determine the School Security Officer assigned to review your submission.
5. ***Summary of project and considerations for reviewer.** Enter a brief description of the project This should be 225 words or fewer.

SmartForm Section: Protocol Team Members

The Protocol Team Members page of the SmartForm should include the names of any individuals involved with the protocol, including those who may need access to this record in the system. Any team members who may have access to data must complete all relevant Information Security Training.

Note: Many types of information security training may be required by the reviewer. The most common required trainings are the Harvard Research Data Security Training Course in the Harvard Training Portal, and the CITI Information Privacy and Security Training at citiprogram.org.

Individuals listed here may also be listed as team members in other systems. This team is specific to data access and management. If a person is not included on this list, or the record is not active, their access to data may be impacted.

In certain instances, reviewers may look to related Agreements or IRB submissions for information about the study team. To add a related submission, Save and Exit the Safety SmartForm to return to the study workspace, then complete the "Manage Related Projects" activity. For more information, see Managing Related Projects. Any related projects will appear on the main study workspace, under the Related Project Tab.

1. **Individuals who will access the data or who are responsible for administration of the project.** Advisors, contractors and collaborators should also be listed here. Harvard Individuals (with a Harvard University ID or HUID) can be selected from a list of names. Begin typing a piece of the person's name in the space provided on the pop up, or you can click the "add" option to search the list of available names. Use the "%" symbol to replace portions of a name of which may be unclear or possibly not spelled correctly. This is called a "wildcard" character. Use the email address column for search or as a guide to selecting the correct person. If the correct person cannot be found via name or email, click the ellipses […]. Choose a Filter by: option to search on a single criteria. Select UserID to search by HUID.

   Only study team members listed here can be designated Principal Investigator Proxies. For more information, see Managing PI Proxy.

   External Individuals can also be listed in this section by entering their first and last name, as well as their institutional affiliation.

   Select Role in Research for each of the Study Team Members added. There are three check boxes to choose from, Can Access Data, Study Support, and Data Custodian. More than one selection can be made for each Study Team Member.

   Important! The person filling in the form will automatically be listed on this page. One should not remove him or herself from this list unless they no longer need access to the submission. Removal from the study team will result in automatic revocation of access.

2. **Attach security or privacy training information as applicable.** Upload documentation for any required information security or privacy training in this section.

   Training may include:
   - **Harvard Research Data Security Training Course** (University-Wide) in the Harvard Training Portal
   - **Information Security Training** in CITI
   - Any additional training as required by Policy or the reviewing School Security Officer.

SmartForm Section: Funding Sources

1. **Will you use funding to purchase additional hardware or technology?** Mark yes if you anticipate costs related to the technology needed to obtain or manage this data. Costs include those for cloud services, vendors, storage, or other service providers.
   Provide additional information about funding used to cover the cost of technology:
   Include GMAS number, if applicable. Describe how any of the costs related to data management will be covered. If your research is sponsored, list any grants that will be used to pay for data management expenses. You do not need to list funding for researcher salaries or other expenses not related to data management.
2. **Will technology expenses be ongoing?** Mark yes if above mentioned expenses are ongoing, no if one-time. The security reviewer may have additional questions regarding this expense.
3. **Does the funding include any additional storage and data management conditions?** Mark yes if there is funding in place to cover additional storage or data management costs.
   If yes, provide a description or additional details about the funding.

SmartForm Section: Data Information

You must add at least one set of data. One or many sets can be listed on this page of the SmartForm.

- **Click Add** to add the following details about one or more data sets.
- Click on the Data Name on the list to view or manage details entered.
- Click the 'x' to the right of the item on the list to remove that entry and all of the details from the form.

1. ***Data set(s) name (Harvard and provider names):** Give the data set (or sets) an easily identifiable name. If the data provider has named the data, it is helpful to use/reference that name in the space provided.
2. ***Data source:** Indicate whether data is internally generated (e.g. data collected by research conducted by the study team), externally provided (e.g. data obtained from another institution), or a combination of both internal and external.

   If external or a combination, search for the source in the drop down menu. If the source is not listed, choose "other" from the list. Type the name of the source in the text box. Provide information about any physical media on which the data will be received.

   Note: if the external source is "Centers for Medicare and Medicaid Services [CMS]," the PI will be required to attest to the use of CMS data as part of the review process. The Safety Specialist/Reviewer for the data safety submission will assign this task to the PI as a required ancillary review.

3. ***Data originates from the following country/countries**: Include any source countries for this data set. Note that country names are in postal code formats (for example "United States" is "USA").
   If USA/United States, state(s), if known. Choose any known source states for consideration in any additional privacy or security requirements which may apply.

4. **Will any of the data be received via physical media such as paper, CD, or external Drive?** If yes, describe the format, method of transfer, and storage location: Provide information to consider as part of the review, including any security measures in place.
5. ***Do you have a contract for use of the data?**
   Mark yes if the data is covered under a data use agreement or other contract. Include the provider number, if there is one.
   Mark no if data will be obtained via other collection methods. Describe the methods, including the use of any survey tools or collection methods.
6. ***Data type description:** Include the type of data being stored, including for example, if it is survey or medical record, as well as the years covered by the data.
7. **Will all of this data be stored or managed at Harvard or otherwise using Harvard resources (e.g. physically on the premises or in Harvard Cloud Storage)?** Mark yes if all data associated with this entry will be stored at Harvard, using Harvard resources, or managed by Harvard researchers.
8. **Harvard Data Security Level:** See https://policy.security.harvard.edu/view-data-security-level for definitions of the Harvard Data Security Levels (DSL). If you are unsure what to select, leave this question blank and work with your assigned School Security Officer to determine the appropriate DSL.
9. ***Places where data will be collected, stored, or analyzed, including tools and locations:** Choose one or more Level-appropriate options from a set of Harvard pre-reviewed tools and locations. Level-appropriate options meet minimum requirements for a Data Security Level (DSL) at or higher than the DSL for the data set(s). Choose "other" if other locations will be written in below. Your School Security Officer will review the appropriateness of your selections for your data set(s).
   - If "other" is indicated, write in all other locations for review.
   - If "other" is indicated OR if the data set DSL is higher than the DSL of one or more chosen places, please also explain any compensating controls or security measures planned.
10. **Will all listed locations be accessed behind HarvardKey or another Harvard-provided authentication?** Mark yes to verify. Mark no if any one of the locations can be accessed in another way.
11. **Are you using encryption to protect the data? If yes**, describe the encryption methods.
12. **Anticipated storage requirements (if available):** Special considerations may need to be made for exceptionally large data sets.
13. **Will data be shared with a third party?** Select yes if any third party may handle, store, collect, transcribe, host the data or application, or otherwise have access to the data, including under a vendor contract for management of the data.
14. **For those doing data analysis, how will output be shared?** Provide a brief description of the ways in which data or results will be shared.
15. **Provide other relevant information about the data.:** Include any details that will support the review or locally required metadata to support data management.

SmartForm Section: Data Access

1. **Methods of data access and collection (mark all that apply)** Select the type of devices the protocol team will use to access the data and whether security on those devices is managed by

Harvard.
If personal computer, mobile device, or tablet are chosen for a project involving the use of DSL3 or DSL4, an attestation and link will display under this section for reference.

2. **Use of data processing applications:** Describe software you plan to use for processing data.
3. **Will the data be linked with other data sets?** If yes, describe the approval and any sets planned for linking, including any potential for re-identification of deidentified data.
4. **Is there a requirement for data destruction?** Some types of data require that data be completely or partially rendered unusable and/or inaccessible after the conclusion of the protocol or a prescribed period.
5. **Additional supporting documents:** Attach any data management plan or relevant information to support the review.
    - Additional information about surveys or data providers may be included here, if applicable.
    - Reference the following site for additional information about Data Management Plans: https://researchdatamanagement.harvard.edu/resources.
    - This form is intended to review information about research data management. Do not upload any research data to the SmartForm.

Important! Once the submission is created and composed, the Principal Investigator must complete the submit activity to send the materials for review. Until the submit activity is executed, the following alert will show under the protocol summary:

> ⚠ **Important!** The submit activity must be completed for review to begin. Only the Principal Investigator, Proxy, or Primary Contact can see and complete the submit activity on the left.

Editing a Submission

You can continue to make changes to a protocol until you submit it for review. You can also make changes if the Safety reviewer requests clarifications or amendments.

To edit a submission before it has been submitted:

1. From **My Inbox**, click the name of the submission to open it
   Note: If the submission does not appear in your inbox, see Accessing a Submission.
2. Click **Edit Protocol** on the left.
   For Amendments, click **Edit Amendment**.
   For Continuing Reviews, click **Edit Continuing Review**.
   For Amendment/CR (amendment with continuing review), click **Edit Amendment/CR**.
3. Make changes as appropriate. When updating a previously submitted document, replace the original document with the revised version. The system will track each version of a file with a revision updated.
4. Exit the submission by clicking the **Exit** link (if prompted, be sure to select **Save Changes & Exit**) or by clicking **Continue** on each page of the form until you reach the final page and then clicking **Save & Exit**.

To edit a submission after it has been submitted:

1. Go to the Submissions page (click **Safety** in the top tab menu).
2. From the All Submissions or In Review tab, click the name of the submission to open it. See [Accessing a Submission](#) for more instructions.
3. Click **Withdraw** on the left side of the page. Completing the Withdraw activity only impacts the submission you are working on and if an Amendment, Continuing Review, or Amendment/CR are withdrawn, it will not impact the status of the main/initial protocol.

   (Optional) On the Withdraw activity pop-up, use the comment box to provide additional information. Do not upload any documents here; protocol documentation should be uploaded to the SmartForm.

   Important! Withdrawing a submission will remove the primary contact and any assigned proxies. To re-add names to these roles, re-complete the Assign PI Proxy and Assign Primary Contact activities, as needed.

4. Click **OK**.
5. The submission will return to the Pre-Submission state, and you can edit as appropriate.
   - When updating a previously submitted document, revise it in tracked-changes format and replace the original document with the tracked-changes version.
   - Exit the submission by clicking the **Exit** link (if prompted, be sure to select **Save Changes & Exit**) or by clicking **Continue** on each page of the form until you reach the final page and then clicking **Save & Exit**.
6. After edits are complete, the PI or PI Proxy must complete the **Submit** activity again, to send it back for review.

Tip: When the submission is in pre-submission or clarifications requested, you may click **Discard** to completely remove a submission from further consideration. Completing the Discard activity only impacts the submission you are working on and if an Amendment, Continuing Review, or Amendment/CR are discarded, it will not impact the status of the main/initial protocol..

Discarded studies (initial submissions only) may still be copied to initiate a new review.

Checking a Submission for Errors

Checking the submission for errors and omissions helps you include all the relevant information, which is critical to ensuring a timely review.

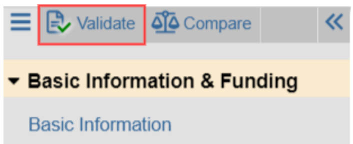
Using these types of error checking helps you supply all the information required for a thorough Safety review:

- **Automatic system error checking** identifies any omitted answers to required questions on the form when you click Continue. A red asterisk (*) precedes each blank or question that requires an answer.

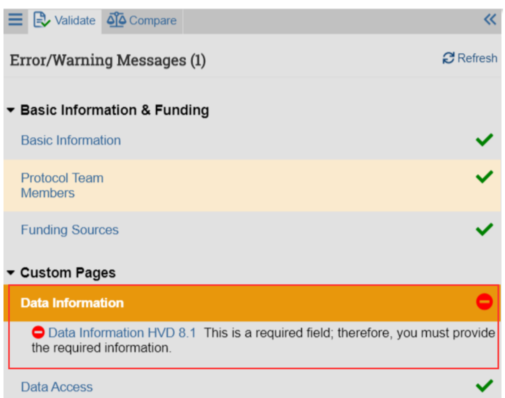
- **Visually inspecting the forms** to see what you may have missed. To perform a visual inspection, open the submission and look through the forms in order. To open the submission, see Editing a Submission. Be sure to answer all relevant questions and attach any helpful documents.
- **Using the Validate option** to find and correct all errors before submitting the study. The system automatically checks for missing required information when the PI attempts to submit the study. However, if you are filling out the forms on behalf of the PI, it is best to check the study for errors before the PI attempts to submit it, using the steps below.

To use Validate to find and correct errors

1. Open the submission, as explained in Editing a Submission.
2. From the left-hand navigation area, click **Validate**.



3. The left-hand navigation area expands to show Error/Warning Messages, listing all the current errors and where to find them.



4. For any error listed, click the link in the error message to go to the form containing the error.
5. Click **Continue** to identify the specific questions on the page with errors.
6. Fill in the missing information.
7. Click **Save** to record your changes and update the list of errors in the Error/Warning Messages pane .
8. Continue correcting errors until no errors are listed.

Submitting Materials for Review

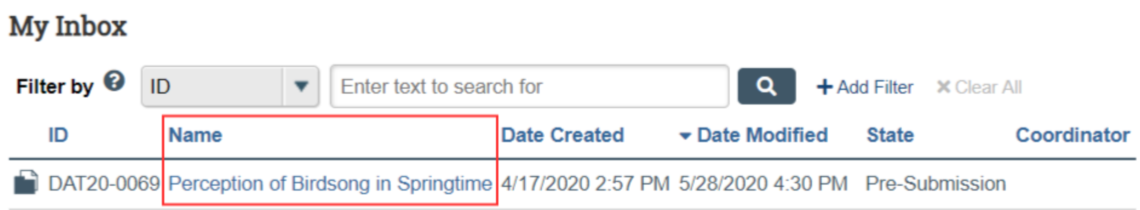
After entering all required information into the SmartForm and attaching files, the Principal Investigator must submit the item for review.

Tip: Check for missing information before attempting to submit, as described in Checking a Submission for Errors. Any errors or omissions not corrected are shown when attempting to submit and must be corrected before you will be able to submit it for review.

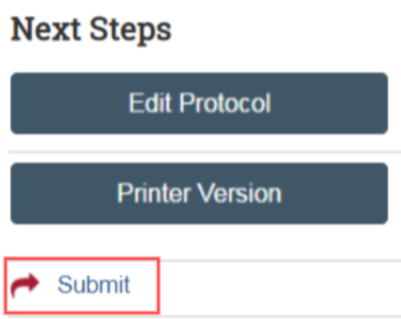
To Submit the Protocol for Review

Important! Only the Principal Investigator can complete the following steps for an initial protocol. Once submitted, the Principal Investigator can assign a Proxy to act on his or her behalf. See [Managing Principal Investigator (PI) Proxy] for more information.

1. Log in to researchsafety.harvard.edu
2. Make sure you are in My Inbox. If you do not see My Inbox, click the **Dashboard** link in the top navigation menu.
3. Click the name of the submission to open it. It should be in the Pre-Submission state.



4. Click the **Submit** button (on the left side of the workspace, under the dark buttons) from the Next Steps list on the left.



   The system will conduct an error check to identify if any required questions were missed. If any errors or warnings are shown, click the link in the Jump To column to go to the page of the SmartForm containing the problem. For more information, see Checking the Protocol for Errors.

   When all errors are corrected, try clicking Submit again.

5. Mark the attestation box on the pop up to agree to the assurance statement presented in the pop-up screen.
6. Click **OK** to complete the activity.
   If you would like to separately refer to the PI assurance statement:
   - Before completing the activity: Click on the Submit button but choose **Cancel** to close the window after reading.
   - Once the Submit activity has been completed: Click on the name of the activity on the History tab of the workspace to read elements of the activity form.

When an initial protocol, amendment, or continuing review is submitted, the PI, PI Proxy, and Primary Contact will receive a notice confirming that the submission has been sent for review successfully.

Submitting your Data Safety and Security project for review initiates a series of activities that may include:

- Notification to and review by a School Security Officer
- Review by relevant Ancillary Reviewer(s)
- Communication about the status of the review to the Investigator

Any of these may lead to a request for the protocol team to take further action, such as providing clarifications or modifying the SmartForm and submission. Whenever the protocol team needs to act, the PI/PI Proxy and Primary contact will receive an e-mail notification, and the protocol will appear in the Dashboard for all protocol team members when they log into the Safety System.

Important! Make sure the appropriate person is listed as the primary contact to receive e-mails and see the protocol in the Dashboard (along with the PI and any PI proxies). See Changing the Primary Contact for more information.

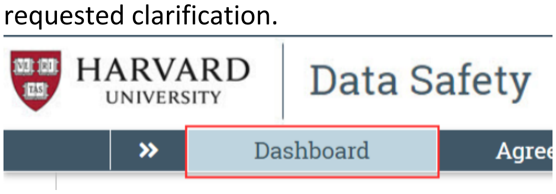
Accessing a Submission

You may want to go to a specific submission workspace to view or update its contents, submit it for review, review it, or take other actions. Note that your access to a submission is personalized based on your role in the system and the role you play in relation to the submission. In addition, the actions you can take on a submission are personalized.

To view a submission workspace, click the submission name when you find it in a list of studies.

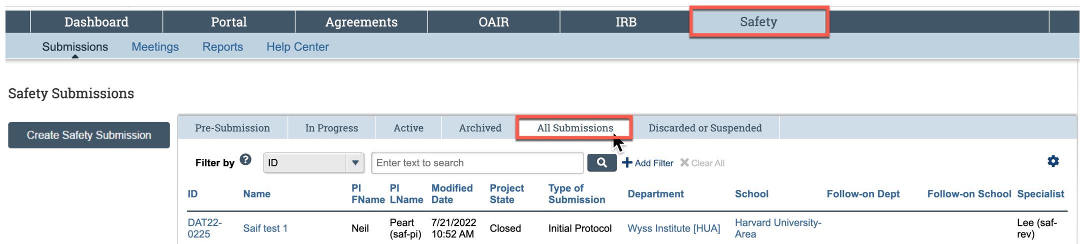
To find a list that includes the submission name:

- **Dashboard** (only items that require attention): Click the **Dashboard** link in the top navigation header. This list displays submissions assigned to you for action, such as submissions you are preparing to submit or submissions that require a response to a requested clarification.



OR

- **Safety** (all items to which you have access): Click **Safety** in the top navigation header and select the **All Submissions** tab. This list displays links to the workspaces for all studies, continuing reviews, and amendments entered into the system that you have permission to view.



Tips:

- Try filtering this list by the protocol name or Principal Investigator. Next to **Filter By,** select **Name** or **Investigator**. Then type the beginning of the name and click **Go.**
- View the **State** column to see where a submission is in the review process.

Managing Submission Permissions

Permissions on a submission are different depending on your role on the protocol. The Principal Investigator, protocol team, and guest permissions are different than School Security Officers and ancillary reviewers. Principal Investigators, protocol team members, and guests have the following permissions:

Action	User Role(s)
Receives system notifications	Principal Investigator, Primary Contact, PI Proxy
Can **create** submissions on behalf of the PI *All types of submission*	Principal Investigator, Primary Contact, PI Proxy, Protocol Team Member
Can **submit initial submissions**	Principal Investigator Only
Can **submit follow-on submissions** on behalf of the PI *Amendments/updates, continuing review, and closures*	Principal Investigator, PI Proxy
Can complete the **Copy Submission** activity	Principal Investigator
Amendment required to add or update this role	Principal Investigator (using amendment to “Other Parts of the Protocol”), Protocol Team Member (using amendment to “Protocol Team Members”). **Note:** The PI Proxy must be a protocol team member, but Proxy assignment does not require an amendment
Has **approval to access data**/is listed on the personnel roster	Principal Investigator, PI Proxy, Protocol Team Member
Has **view-only** access to the submission	Guest

** To manage permissions per project, see sections for how to change a primary contact, assign proxies, change protocol team members, copy a protocol, and add guests.*

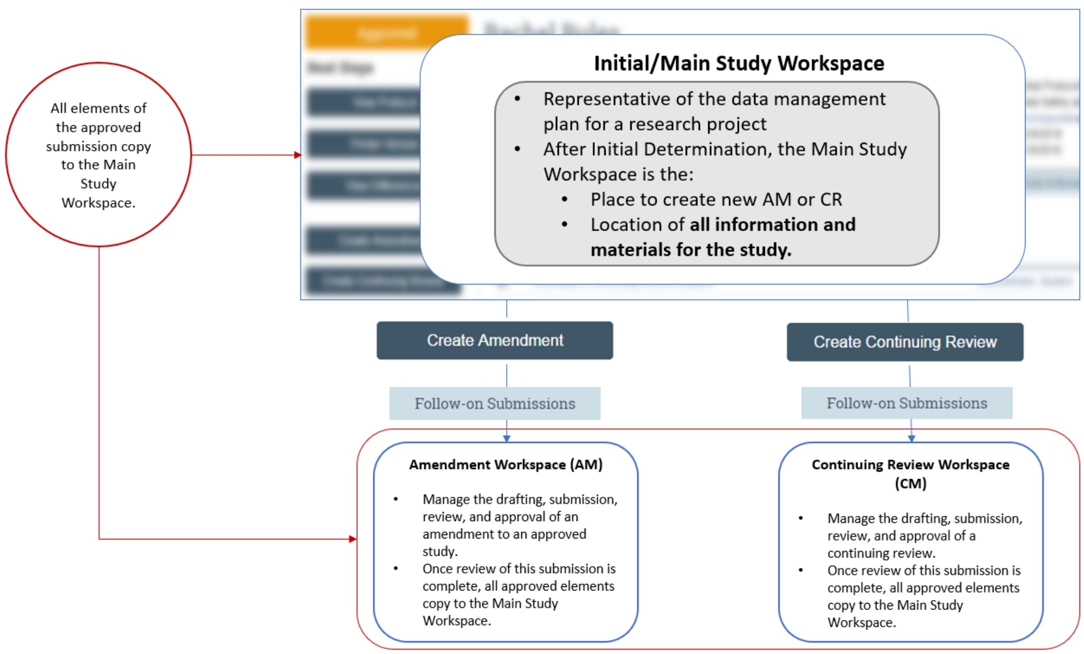
*** For view access to many records in a department or school, see [Requesting Viewer Access to ESTR-IRB, Agreements-DUA, or Data Safety]() for expanded guest access.*

Important! Guest access is managed separately for each protocol, amendment, and continuing review. Granting a user access to the protocol will not automatically give them access to any related amendments or continuing reviews.

Submission Workspace Overview

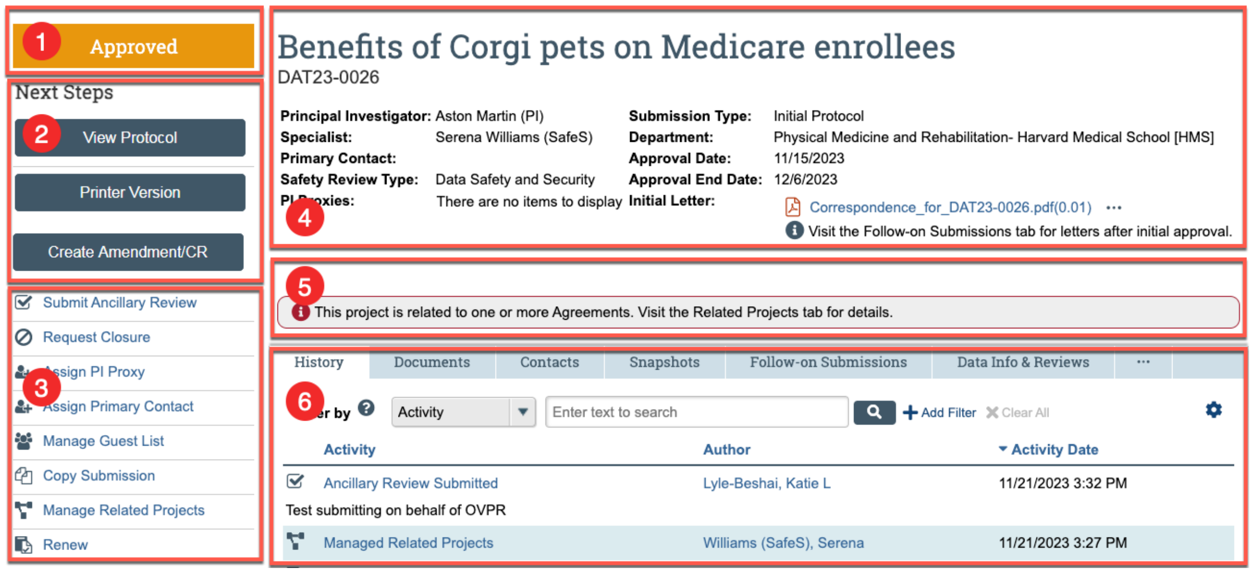
The Initial/Main Study, Continuing Review, and Modification/Update workspaces are formatted similarly. The following general concepts apply to navigation:

- The Initial/Main Study workspace (labeled DAT##-####) always has the most current approved information and materials for a protocol.
- Continuing Review, Amendment, and Amendment/CR (not depicted in the image below) workspaces are used actively during the review of that submission only. Once a determination is made (or the submission is discarded), the Initial/Main Study workspace is updated with any revised elements and these workspaces are used for reference only and should not be the go-to location for protocol information.



Workspace Regions

Image displays the Initial/Main Study workspace for reference



Region	Information in this region
1	**Status** Visible in all workspaces, the status region will show the current review status of the submission.
2	**Next Steps** Visible in all workspaces, this set of blue buttons allows for: • Editing or viewing the current submission SmartForm, • Displaying a printer-friendly version, • Viewing changes over time, and • On Initial/Main study workspaces only: Creating new Continuing Review or Amendment submissions for the study by choosing Amendment/CR.
3	**Activities** Visible on all workspaces, activity buttons display depending on the type of submission, the status of the submission, and your role on the study. Mostly, activities displayed take action on the submission only. However, Assign PI Proxy, Assign Primary Contact, and Manage Guest List are only visible on the Initial/Main study workspace.
4	**Submission Overview** This section displays the following submission-specific items for reference: • Number and name of the submission/workspace being viewed • PI, submission type, primary contact, PI Proxy/ies (if assigned), and review specialist (if assigned) • Review determination letter (labeled “Letter”) if a determination has been made. • On Continuing Review, Amendment, or Amendment with CR workspaces only: a link to the Initial/Main study will appear at the top of this section.
5	**Notification Area** When the record has not yet been submitted for review, a reminder to complete the submit activity displays in this space.
6	**Submission Tabs** On a submission, the Initial/Main study workspace shows all current approved details (including documents and study team members) while all follow-on

submission workspaces display information that was proposed at the time of review and determination. Click the tabs to view:

- History Information about each action taken on a submission and in-brief view of comments.
- Documents All documents submitted for review, with versioning information for each document.
- Contacts List of study team members listed on the SmartForm, including current training information on file.
- Snapshots View of the application at each change in state (for example, the appearance of the SmartForm between Specialist Review and changes submitted).
- Follow-on Submissions Links to Continuing Review, Amendment, or Amendment/CR workspaces for a study (only visible on the *main study workspace*). For easy reference, the tab also displays the name of the assigned specialist for each of the follow-on submissions.
- Data Info & Reviews Displays each data set described within the submission, its Harvard Data Safety Level, and all corresponding data storage locations. Also displays the information that is relevant for external reviewers who need to access basic information about the record.
- Related Projects Quick links to any submissions in the ESTR-IRB and Agreement-DUA system that are related to the submission you are viewing. Related projects should be added or removed by using the **Manage Related Projects** activity.

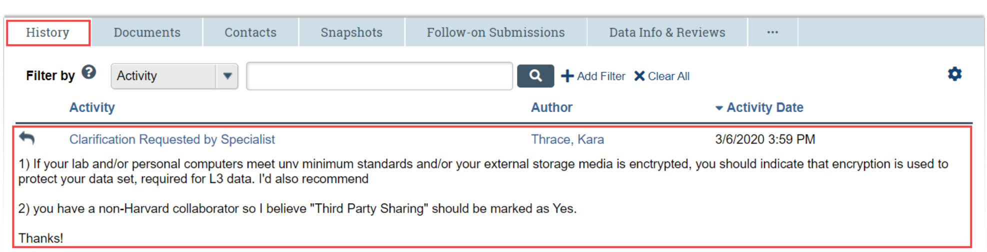
Responding to a Request for Clarifications

At any stage during the review process, the reviewer may request clarifications to the protocol. The PI, any PI Proxy, and the protocol's primary contact will receive a system notification requesting clarifications. The protocol also appears in My Inbox for each member of the protocol team.

Important! Any protocol team member can make changes to the protocol and submit a response (except for the Primary Contact). Failure to respond promptly slows the review process for your submission.

To view the details of the request and respond with the changes:

1. From the **Dashboard**, click the name of the protocol to open it.
2. Locate the details of the request, as described here:
3. In the Activity column under Clarification Requested, read the request details. If applicable, click the **read more** link to display the remaining text.

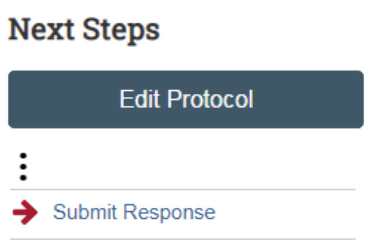


4. Edit the protocol to incorporate the changes as needed. For instructions, see Editing a Submission.

Notes:

- In most cases, you can update all aspects of the protocol, including adding, updating, or removing attached documents.
- When updating a previously submitted protocol document, revise it in tracked-changes format and replace the original document with the tracked-changes version.

5. Click **Submit Response** to return the protocol to the reviewers. Click **OK**. The protocol returns to the review process.



Note: The Submit Response form gives you space to type a point-by-point response to the requests and to attach a file. However, any permanent protocol information should be incorporated into the SmartForm itself.

Changing Documents on a Protocol

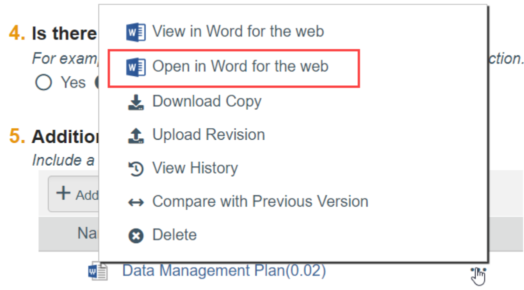
You may need to modify a protocol's documents when:

- A reviewer requests changes prior to approval
- Submitting an amendment to an approved protocol.

To change documents prior to protocol approval

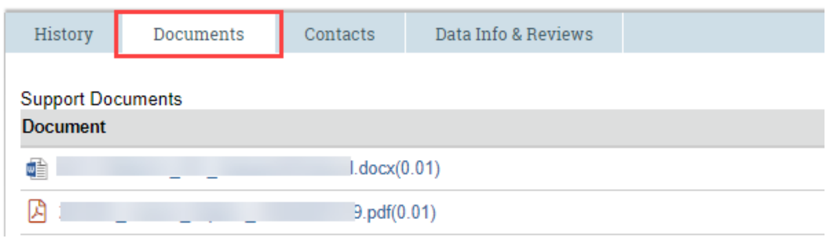
There are two ways to change documents (when the submission is in an editable state).

A. Edit the document directly in Office Online
Note: This option is only available for Microsoft XML documents (file extensions .docx, .xlsx, .pptx, and .vsdx).
1. From the **Dashboard**, click on the name of the submission to open the workspace.
2. Click Edit Study on the left. For amendments, click Edit Amendment. The SmartForm will open.
3. Click the Update button to the left of the document
4. Click the ellipsis next to the document and select the **Open in word for the web** option



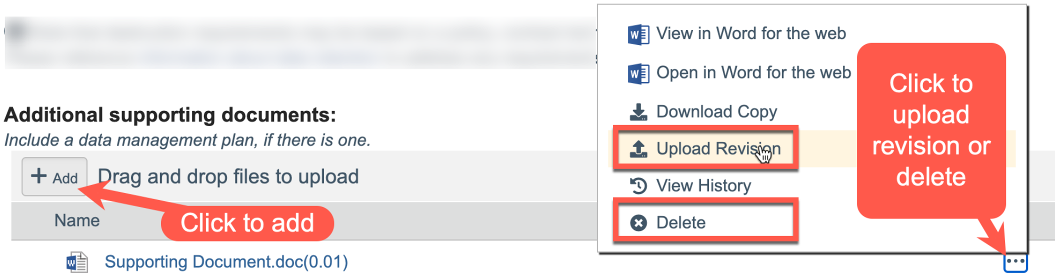
5. The document will open in Office Online in a new tab. Make edits, enabling the Tracked Changes feature as needed, and close the tab once you have finished editing. Changes to the document will be saved automatically.
6. Complete any further updates and submit the changes for further review. See the section Editing a Submission for further details.

B. Download a copy and upload a new version
1. From the **Dashboard**, click the name of the submission to open the workspace.
2. Click the **Documents** tab.



3. Click the name of the document in the Document column and save it to your computer.

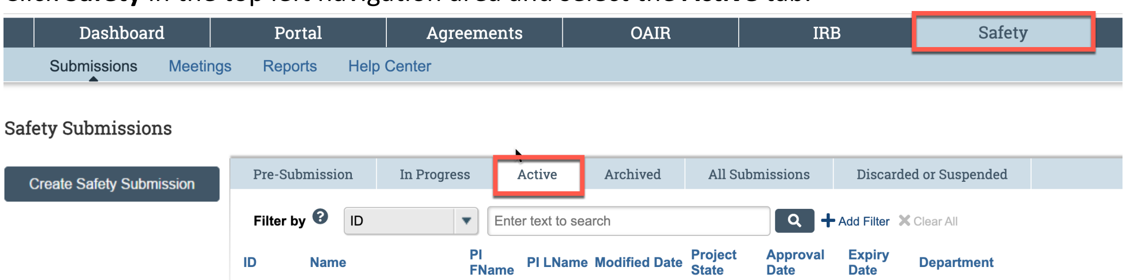
4. Open the saved document and make edits. Enable the Track Changes feature as needed.
5. When finished with your changes, save the revised document on your computer.
6. Go to the submission workspace and click **Edit Protocol** (or Edit Amendment or Edit Amendment/CR) on the left.
7. Navigate to the location of the current document within the SmartForm by clicking Continue on the right.
8. Replace the original protocol document with the revised version by clicking **Update** beside the document on the SmartForm or use other controls to make document changes.



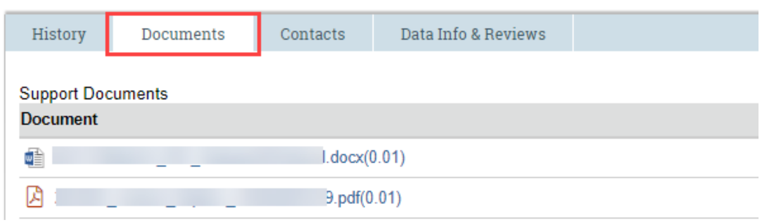
9. Complete any other updates and submit the changes for review. See the section [Editing a Submission]() for further details.

To change documents on an approved protocol

1. Click **Safety** in the top left navigation area and select the **Active** tab.



2. Click the name of the approved protocol.
3. Click the **Documents** tab.



4. Click the document in the **Document** column and save it to your computer. In some cases, this document may contain previously approved tracked changes and comments. To update contents to match the current final-approved version, use the review features in Word to accept all changes and remove any comments. Use this clean document as a starting point for your revisions.

5. Open the saved document and make edits. Enable the Track Changes feature as needed.
6. When finished with the changes, save the revised document to your computer.

7. Go to the approved protocol workspace and create an amendment to update the SmartForm and submit the proposed changes for IRB review. See the section on Creating a Follow-On Submission after Protocol Approval for further details.

Communicating with Staff During Review

During and after the review of a protocol, you can complete the **Add Comment** activity to post a note to the submission history that all individuals with access to the submission may view.

In the activity, pop up: choose the Safety Specialist as a notice recipient to also notify the assigned specialist.

3. Who would receive an e-mail notification:
Only choose 'safety specialist' if a person is assigned to this review.

	Role Name
☐	PI/PI Proxies/Primary Contact
☐	Protocol Team Members
☐	Safety Specialist

Important!

- The information in these activities is visible to all individuals with access to the submission, even if they are not selected as notice recipients.
- Do not attach items which are part of the review
- If a submission is in the Clarifications Requested state, use the **Submit Response** activity to send information back to the reviewers.

Managing Related Projects

When a submission has other associated records in Data Safety, ESTR, and/or Agreements, completing the Manage Related Projects activity will connect the records across the systems so the reviewer may consider the status of associated records and any additional context of these associated records in the review.

This activity can be completed by the PI, PI Proxy, Primary Contact and members of the project team at any time in the review process.

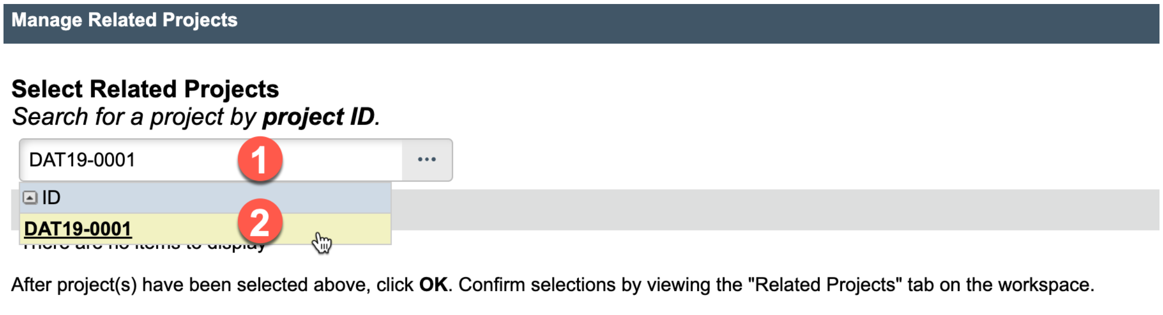
To Manage Related Projects

1. On the main protocol/study/agreement workspace (marked in the center as "Submission Type: Initial Protocol"), click the **Manage Related Projects** activity.

   Manage Related Projects

2. In the pop up, search for the related project by typing or pasting the its complete ID number into the search box (1). When it appears below, highlighted in yellow, click on the ID to choose the submission (2). You can also click the ellipses […] to search the list of available submissions. One or more selected project(s) will appear on the list in the pop up.

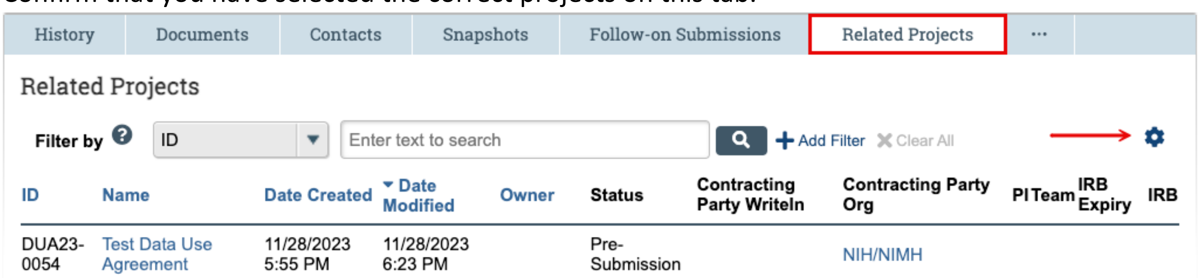
Note: You may only search for submissions to relate by their IDs.



3. **Click OK** to create the relationship between projects and return to the workspace.

Click on the "Related Projects" tab of your protocol workspace to view related projects. Additional details about related projects will appear, including ID, name, state, date modified, and a link to the workspace of the related project. Related projects can be sorted, filtered, and exported as .csv by clicking on the gear symbol to the right of the **Add Filter** button.

Confirm that you have selected the correct projects on this tab.

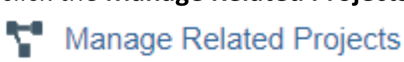


Important! Notes about using Manage Related Projects

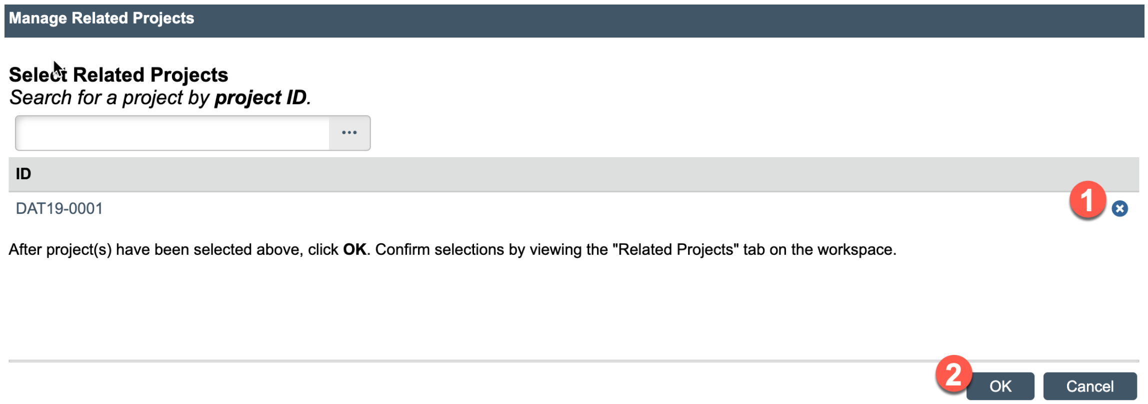
- Relationships between projects are bi-directional. Once you have created a relationship between projects, it will appear (within a few moments) on the "Related Projects" tab for both submissions. You do not need to manage the relationship in both places.
- You may only create relationships between two initial/main studies. Follow-on submissions (such as amendments and continuing reviews) are not available for selection.
- Project states may not update automatically. The correct state will always be displayed on the workspace of that project.

To remove a relationship between projects using the "Manage Related Projects" activity

1. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol"), click the **Manage Related Projects** activity.



2. Remove projects by clicking on the "X" at the far right of the entry (1).

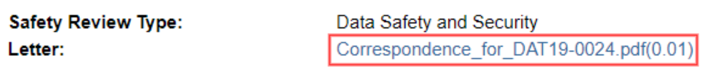


3. **Click OK** (2) to confirm the removal and return to the protocol workspace.

Finding Determination Letters and Documents

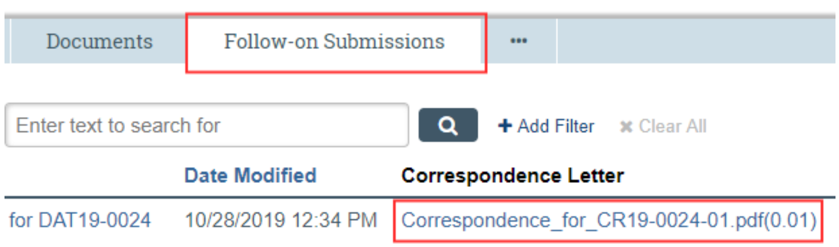
To find determination letters

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved submission (See [Accessing a Submission]() for more instructions).
3. View the determination letter at the top right of the workspace.



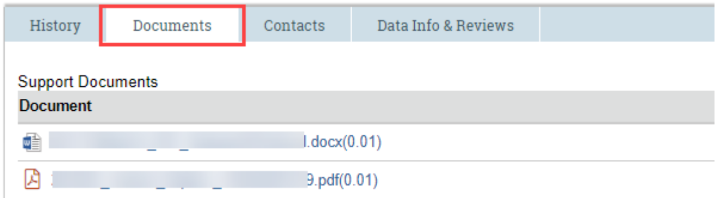
OR

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved submission (See [Accessing a Submission]() for more instructions).
3. Click the Follow-on Submissions tab and click the Correspondence Letter link to see any/all Amendment or Continuing Review letters. To **view** a letter, simply click on any Correspondence link. To **save** a letter, right click and select “Save Link As.”



To find current protocol documents

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved submission (See [Accessing a Submission]() for more instructions).
3. Click on the **Documents** tab on the main protocol workspace.



4. Click on the appropriate document link to view the version you're looking for. To save a document, right click and select "Save Link As."

Managing Principal Investigator (PI) Proxy

The Principal Investigator may assign proxy permissions so that system activities only available to the PI can be completed by another member of the study team. The PI Proxy must be a member of the study team.

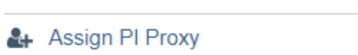
The purpose of assigning a system-based proxy is to assist with the management of follow-on submissions (Amendment and Continuing Review or Closures). PI Proxy permissions do not imply that the named Proxy has PI responsibilities.

A PI Proxy can only be assigned by the PI or an existing PI Proxy. The Proxy can be assigned after initial submission but before the initial approval. Once a PI Proxy has been assigned, the Proxy:

- Can submit follow-on submissions and protocol materials on behalf of the PI.
- Will receive all system notifications pertaining to the protocol.

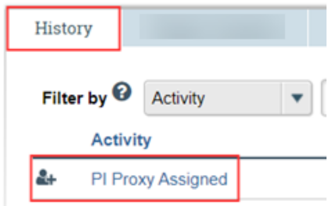
To assign a PI Proxy

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See Accessing a Submission for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), under Next Steps, click **Assign PI Proxy**.



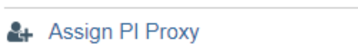
4. A pop-up will appear where you can select the individual(s) you would like to designate as PI Proxy by clicking on the ellipses […] beside the space to enter a name. The secondary pop-up list will show only approved protocol team members. If an individual you wish to assign as PI Proxy is not listed, they first must be added to the protocol via an approved Amendment.
5. Check any/all of the individuals you wish to make PI Proxy and review the assurance statement.
6. Click **OK**.

All updates to PI Proxy will be recorded on the main protocol workspace, capturing the name, date, and time that the PI completed the activity and serving as record of the PI assurance of compliance. To review the PI assurance that appears on the activity form, click on the activity name in the History.



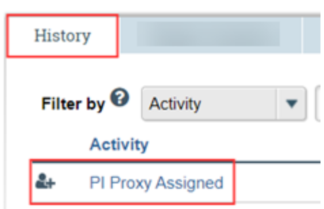
To remove a PI Proxy

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See [Accessing a Submission]() for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), under Next Steps, click **Assign PI Proxy**.



4. A pop-up will appear where you can deselect the individual(s) you would like to remove PI Proxy permissions from.
5. Uncheck any/all of the individuals you wish to remove PI Proxy permissions from and review the assurance statement.
6. Click **OK**.

All updates to PI Proxy will be recorded on the main protocol workspace, capturing the name, date, and time that the PI completed the activity and serving as record of the PI assurance of compliance. To review the PI assurance that appears on the activity form, click on the activity name in the History.



Important! Any PI Proxy that is removed from the protocol via an Amendment to protocol team members will automatically lose PI Proxy permissions.

Changing the Primary Contact

By default, in addition to the PI and PI Proxy, the Primary Contact is a recipient of all system emails (including determination notifications and when the reviewer requests clarifications). Changing the Primary Contact does not require an amendment. Making this change takes effect immediately and can be changed at any time. For example, it may help to provide a contact person in addition to the PI if the PI does not check e-mail frequently. The Primary Contact can also edit the protocol just as a protocol team member can.

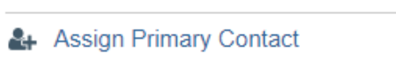
Notes:

- The person who creates the initial submission is assigned as primary contact by default and is automatically listed on the Protocol.
- The primary contact cannot take any actions on behalf of the PI. Only members of the protocol team can propose changes, submit response to clarification requested, and only a PI Proxy can submit a follow-on submission.
- To change the primary contact, you must be the current primary contact, a member of the protocol team, or the School Security Officer assigned to the protocol.
- The Primary Contact may be assigned while completing the SmartForm, on the Basic Information page or via activity.
- The PI and PI Proxy continue to receive notifications regardless of the Primary Contact assignment.
- Amendment, Amendment/CR or Continuing Review will have the same Primary Contact as the Initial Protocol. To change the Primary Contact on these submissions, do so in the main protocol workspace.

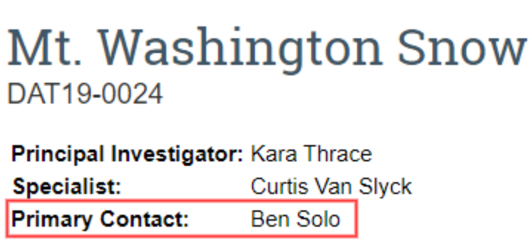
Important! The person who creates the initial submission is assigned as primary contact by default and is automatically listed as part of the study team. In order to ensure continued access to the submission, do not remove the primary contact from the list of study team members.

To change the Primary Contact

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See [Accessing a Submission]() for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), under Next Steps, click **Assign Primary Contact**.



4. A pop-up will appear where you can select the individual(s) you would like to designate as Primary Contact. Begin typing the name of the new contact. A list of matching names will appear. Click on the correct name. The name should now appear as a blue link in the space provided.
5. Click **OK**. You will be directed back to the main protocol workspace, and the Primary Contact will be updated in the top part of the page:

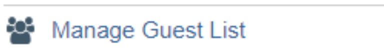


Managing Guests with View-Only Permissions

During the course of a project, you may want to add a guest who can view your protocol and its documents. Guests have view-only permissions and cannot make edits to the protocol or create follow-on submissions. Adding/removing a guest does not require an amendment to the protocol.

To add/remove a guest to the protocol:

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See Accessing a Submission for more instructions).
3. On the main protocol workspace (marked in the center as “Submission Type: Initial Protocol), under Next Steps, click **Manage Guest List**.



4. A pop-up will appear where you can review the list of people who can view the protocol without being on the guest list.
5. To **add a guest**, begin typing the name of the new contact in the search box at the bottom. A list of matching names will appear. Click on the correct name.
6. To **remove a guest**, click **Remove** on the right, next to their name.
7. Click **OK**.

Copying a Protocol

Over the course of submission and review, it may be appropriate to copy the elements of one protocol into a new submission, which then can be edited and submitted for review. For example, it may be appropriate to copy a protocol if:

- There are basic elements of a protocol (such as the list of protocol team members) that are similar to a new project that will be proposed,
- A protocol was discarded in error, or
- A School Security Officer requests that you copy the protocol.

Copying a submission will replicate all information on a protocol (including document) into a new submission. A protocol can be copied at any time.

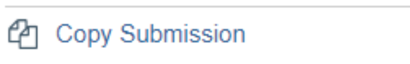
However, note that:

- The status of the copy is completely independent of the status and management of the original protocol.
- Only a Main/Initial Protocol can be copied. Other submissions (for example, Amendment or Continuing Review) cannot be copied.
- Only the PI can copy a protocol.
- The new copy must be further edited and submitted by the PI.
- If the copy was created in error, it can be discarded.

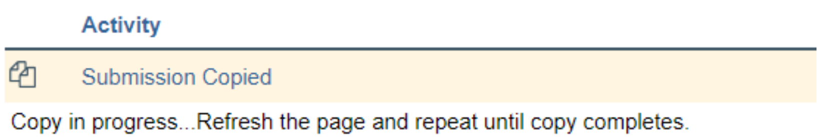
Important! Do not copy a protocol to propose changes to an active project or to request continued review. See Creating a Follow-On Submission after Protocol Approval for instructions to create an amendment, continuing review, or protocol closure for an active project.

To copy a protocol:

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See Accessing a Submission for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), under Next Steps, click **Copy Submission**.



4. Write in the name of the new submission (this can be edited after the submission is created).
5. Click **OK**.
   The copy activity will appear under the History tab of the protocol workspace. While the system is creating the copy, a progress note will appear:



6. Navigate to the new protocol by either refreshing the page to view and click on a link to the new copy, or clicking on My Inbox in the top navigator bar and clicking on the new submission.
7. Complete steps to edit the submission and submit it for review (see Editing a Submission for more instructions).

Requesting Changes or Extension after Initial Approval

All submissions associated with a protocol after the initial creation are called "follow-on" submissions. These include Amendment, Continuing Review, and Amendment/CR (amendment with continuing review) submission types.

Complete the Renew Activity to Extend the Approval Period

Use the renew activity for approved (not lapsed) projects, when a researcher is able to confirm that there are no changes to a protocol and no incidents have occurred in the last year. Upon successful completion of the activity, the approval end date is extended, and a confirmation notice is sent to the PI, Primary Contact, and proxies.

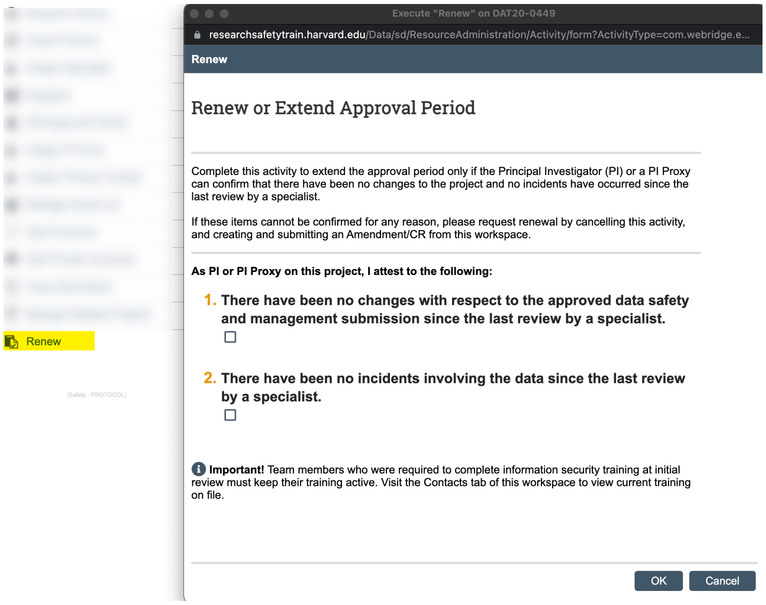
Important! Only the Principal Investigator (PI) or a PI Proxy can confirm that there have been no changes to the project and no incidents have occurred since the last review by a specialist.

To Renew a project:

1. Navigate to an approved protocol (See Accessing a Submission for more instructions).

2. Click on the Renew activity on the left-hand side of the workspace.

3. Review the check box options to attest that there have been:
   - No changes with respect to the approved data safety and management submission since the last review by a specialist; and
   - No incidents involving the data since the last review by a specialist.



4. Click on "OK" to complete the Renew activity.

Note: Researchers can still use Amendment/CR to request changes, share specific updates on approved projects, or request renewal of lapsed projects.

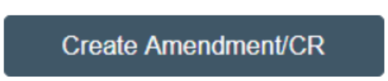
Submitting an Amendment to an Active Protocol

Making any changes to an approved protocol will require an amendment that must be reviewed before changes can go into effect.

Important! Updating the SmartForm does not send the submission for review. The PI or PI Proxy must click **Submit** (on the left, in the submission workspace) for the submission to proceed to the next state of review.

To create and submit an Amendment to an active project

1. Log in to researchsafety.harvard.edu.
2. Navigate to an approved protocol (See Accessing a Submission for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), click the **Create Amendment/CR** button.



4. Select the type of submission preferred
   - **Amendment:** to only propose changes to an active protocol

  - **Amendment/CR:** to both propose changes and extend the approval period for an active protocol
  - **Continuing Review:** to only extend the approval period for an active protocol
5. After choosing Amendment or Amendment/CR, choose one or both types of amendment on the first page of the SmartForm.
   Note: Only one amendment of each type may be open at a time.
   - **Protocol team member information** allows for updates to responses to funding questions, and the addition and removal of protocol team members and updates to protocol team member-related documents (such as training certificates).
   - **Other parts of the protocol** allows for revisions to:
     - The Principal Investigator
     - Any other section of the SmartForm, including information about Data Sets, and Data Access.
6. By selecting "Continue," the system will guide you through some questions about the requested change and take you to a copy of the SmartForm. Refer to the What to Include in the Protocol SmartForm section for additional instructions relative to proposed changes to the approved protocol.
7. Follow the remaining steps to Edit a Submission or click **Save & Exit** when edits are complete. You will be returned to the submission workspace.
8. The PI or PI Proxy must click **Submit** (marked with a red arrow) for the submission to proceed to review.

Tips:
- To change the Principal Investigator on an approved protocol, select the "Other parts of the protocol" amendment scope.
- Once an amendment scope is selected and saved, it should not be changed on that submission.

Submitting a Continuing Review

Your safety submission must be updated and reviewed annually or by the expiry date noted during a previous review. The PI, PI Proxy, and Primary Contact will receive notice of an approaching continuing review deadline in advance of protocol expiry. If the protocol indicates an expiration date or you receive notifications from the system, submission of a continuing review request is required to maintain approval. Failure to submit a Continuing Review prior to expiry may impact data access.

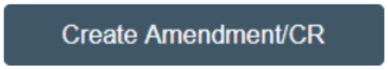
This submission is only used to provide an update when required. Changes to an existing protocol must be proposed via a separate amendment submission. Please see the section on Submitting an Amendment to an Active Protocol for steps to complete an amendment.

Important! Updating the SmartForm does not send the submission for review. The PI or PI Proxy must click **Submit** (on the left, in the submission workspace) for the submission to proceed to the next state of review.

To create and submit a Continuing Review for an active project

1. Log in to researchsafety.harvard.edu.

2. Navigate to an approved protocol (See [Accessing a Submission](#) for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol"), click the **Create Amendment/CR** button.



4. Select the type of submission preferred
   - **Amendment:** to only propose changes to an active protocol
   - **Amendment/CR:** to both propose changes and extend the approval period for an active protocol
   - **Continuing Review:** to only extend the approval period for an active protocol
5. Complete the Continuing Review Information SmartForm Pages. Click **Continue** to proceed through the SmartForm and answer all questions. When you reach the end of the SmartForm, click **Save & Exit**.

Closing a Protocol

To submit a protocol closure request:

1. Log in to [researchsafety.harvard.edu](#).
2. Navigate to an approved protocol (See [Accessing a Submission](#) for more instructions).
3. On the main protocol workspace (marked in the center as "Submission Type: Initial Protocol), under Next Steps, click **Request Closure**.

4. Complete the required questions on the Activity Form and click **OK**.

The School Security Officer or assigned specialist will review your request for closure and, if appropriate, close the protocol. The Principal Investigator, PI Proxy, and Primary Contact will receive a system notification when the protocol is closed.

Generating Standard Reports

The Safety system includes many standard reports to help you find relevant submissions and understand the overall data safety and security program.

The reports provide links to the individual submissions, as well as sorting and filtering options.

Any user has access to reports, but the data in the reports is limited to the studies visible to the individual. For example, a report generated by a PI will only include studies that person is allowed to see elsewhere in the system: studies for which the person is included on the study team or guest list. School Security Officers and other administrators may have access to all report data.

To generate a standard report:

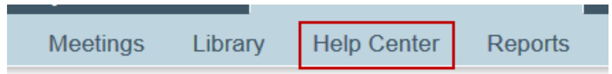
1. Log in to [researchsafety.harvard.edu](#).
2. Click **Safety** in the top navigator.

3. Click **Reports** in the Safety sub-menu.
4. The list of standard reports appears. Identify the report you want to generate and click the title. The report will appear, listing the relevant submissions.
5. Report results can be exported to Excel from the results pop-up window by clicking the **Export** button.

Important! Notes on Exporting Reports

- Click the Export option once. The system will take a moment to indicate the download has occurred.
- If the download does not appear automatically, check to confirm that your browser is not saving files to a default folder.
- If no other exports are pending, the progress with display on the button and a download option will appear when the export file is ready for download.

Finding More Information

Resource	Description	How to Access It
Help for a field or page	More information about a question or form.	Click the question mark icon next to the question or at the top of the form.
Help system	The full online help system, with search and table of contents. The online help contains procedures and information for all users.	Click the **Help Center** sub-menu link at the top of the screen. 
Safety Submission Guide	Instructions for submitting a protocol for review.	Click the **Help Center** sub-menu link at the top of the screen. On the Guides tab, click the name of the guide to open it.
Safety Reviewer / Specialist Guide	Instructions for reviewing a submission.	
Data Safety Support	External website with additional information about using the Safety system	https://ras.fss.harvard.edu/data-safety
Data Safety Help Desk	Contact for help with access and use	rshelp@harvard.edu
OVPR, HUIT and Support Websites	Information about the review process and requirements	▪ Office of the Vice Provost for Research: https://research.harvard.edu/2020/06/26/research-data-management/ ▪ Harvard University Information Technology: https://security.harvard.edu/ ▪ Research Data Management at Harvard: https://researchdatamanagement.harvard.edu/

This guide was created and edited by Harvard University based on materials originally produced by Huron Technologies, Inc.

Appendix I: System-wide Permissions

The following table describes which submissions a user has access to, based on role.

All individuals with a HarvardKey have access to the Safety Submission. Users must have a HarvardKey in order to be assigned a role by a study team member or administrator.

<table>
<tr><th>Role</th><th>Access Summary</th></tr>
<tr><td>School Security Officer (Specialist)</td><td>Can access all submissions
Can view lists of submissions, filtered by area
Can review/approve submissions
The assigned specialist can provide study team support (can edit the submission on behalf of the study team when in an editable state)</td></tr>
<tr><td>Resource Manager</td><td>Read-only access
Can view all submissions where the resource has been chosen on the SmartForm</td></tr>
<tr><td>School/Department Viewer</td><td>Read-only access
Can view all submissions across the suite of applications (including ESTR-IRB and DUA-Agreements submissions) where an associated department has been chosen on the SmartForm</td></tr>
<tr><td>Principal Investigator (PI)</td><td>Can manage (view and edit, depending on state) all submissions for which the user is listed as Principal Investigator)
Can Submit Initial Submissions for review
Can assign a PI Proxy to act on their behalf</td></tr>
<tr><td>Principal Investigator (PI) Proxy</td><td>Can manage (view and edit, depending on state) all submissions for which the user is listed as Principal Investigator)
Can Submit amendments and continuing reviews on behalf of the Principal Investigator
Note: The PI Proxy must be a member of the study team.</td></tr>
<tr><td>Study Team Member</td><td>Can manage (view and edit, depending on state) all submissions for which the user is listed as a study team member)
Note: The submission creator is listed as Primary Contact and added to the study team automatically. The Primary Contact must be a member of the study team to retain access to the submission.</td></tr>
</table>

Appendix II: List of School Security Officers by School/Department

The Data Safety system automatically assigns a school security officer upon the submission of a protocol, amendment, or continuing review based on the Responsible Department selected on the first page of the SmartForm. This person is referred to as a "Specialist" within the application.

As some schools have multiple school security officers, the system may automatically assign the submission to a department, to be triaged to an individual specialist for completion of the review.

For more information, see [Information Security Officers by School](#).

School	**Assigned Specialist**
Central Administration (CADM)	Harvard University IT (HUIT)
Faculty of Arts & Sciences (FAS)	Harvard University IT (HUIT)
Graduate School of Arts & Sciences (GSAS)	Harvard University IT (HUIT)
Graduate School of Design (GSD)	Hal Gould
Harvard Business School (HBS)	HBS Information Security
Harvard Divinity School (HDS)	Dan Hawkins
Harvard Graduate School of Education (HGSE)	Sarah Pruski
Harvard Kennedy School (HKS)	Ramon Delacruz
Harvard Law School (HLS)	Matt Hernandez
Harvard Medical School (HMS)	Joe Zurba Caroline Wood (Healthcare Policy)
Harvard School of Dental Medicine (HSDM)	Joe Zurba
Harvard School of Public Health (HSPH)	HSPH Information Security
School of Engineering and Applied Sciences (SEAS)	Judit Flo Gaya
Wyss Institute	Joe Zurba

Appendix III: List of Certified Resources

The following resources are available for selection as Data Storage Locations in the Safety application. Visit the Harvard Information Security and Data Privacy website for resources on handling data and devices surely at Harvard.

Name	Certified for DSL
HMS HCP (Markley)	4
HBS Accellion (Secure File Transfer)	4
HMS HCP (180 Longwood)	4
Harvard Confluence or Wiki (non-public, behind HarvardKey)	3
HBS O365 OneDrive	3
HSPH RedCap (via Partners)	3
Harvard O365 SharePoint (HRCI) by special request only	4
Harvard Google Drive (g.harvard)	3
Harvard O365 Outlook	2
Harvard O365 SharePoint	3
Harvard O365 One Drive	3
Harvard Office Message Encryption (OME)	4
Harvard DropBox	3
Harvard Canvas LMS	3
HGSE Kaltura Video Hosting (Canvas and Sharepoint (HRCI))	4
HBS O365 SharePoint	3
HGSE NextCloud	4
HBS Qualtrics	3
Harvard-MIT DataCenter (HMDC-HCRI) by special request only	4
HGSE CEPR Secure Data Environment	4
HBS Research Computing Storage and Compute Cluster	4
HMS RedCap	4
Harvard Zoom	3
HSPH CPDS Data Enclave	4
Harvard O365 Forms to SharePoint	3
Harvard Qualtrics	3
Harvard Accellion Kiteworks (Secure File Transfer)	4
Harvard Laptop	3
HMS O2	3
Harvard Google Transcription	3
FASRC Cannon Cluster (previously Odyssey)	2
FASRC Secure Environment (consultation required)	3
IQSS Research Computing	3
Harvard-MIT DataCenter (HMDC)	3
HBS Research Computing MariaDB RDBMS	4