

Qualtrics Survey Privacy Policies

Washington University has strict rules about the kind of data that may be collected and how it may be used given our limited Business Associates Agreement (BAA) with Qualtrics. This guide is intended to help survey creators better secure their data and reduce security risk through the use of available security and privacy settings. Guidance is provided on:

- What is PHI?
- What is PII?
- Where to access Security & Privacy Settings
- Privacy Setting Descriptions
- Privacy Setting Use Cases

What is Protected Health Information (PHI)?

PHI is Protected Health Information that this produced, saved, transferred, or received in an electronic form (such as email or text).

- Protected Health Information is the combination of health information with one or more of the designated HIPAA identifiers
- An email address or telephone number is a HIPAA identifier

Health information includes information about:

- an individual's past, present or future physical or mental health or condition
- the provision of health care to an individual
- the past, present, or future payment for the provision of health care to the individual

What are the HIPAA identifiers?

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
 - The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people
 - The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

- Telephone numbers
- Facsimile numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Photographs/Videos
- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

Find out more about HIPAA policies at <https://hipaa.wustl.edu/resources/hipaa-identifiers/>.

What is Personally Identifiable Information (PII)?

PII refers to personally identifiable information (PII). This information includes an individual's first and last name or their first initial and last name with any other data element.

PII must be protected from unauthorized access, disclosure, or public release to prevent adverse outcomes such as identity theft, legal and reputational damage, or compromise to systems and accounts.

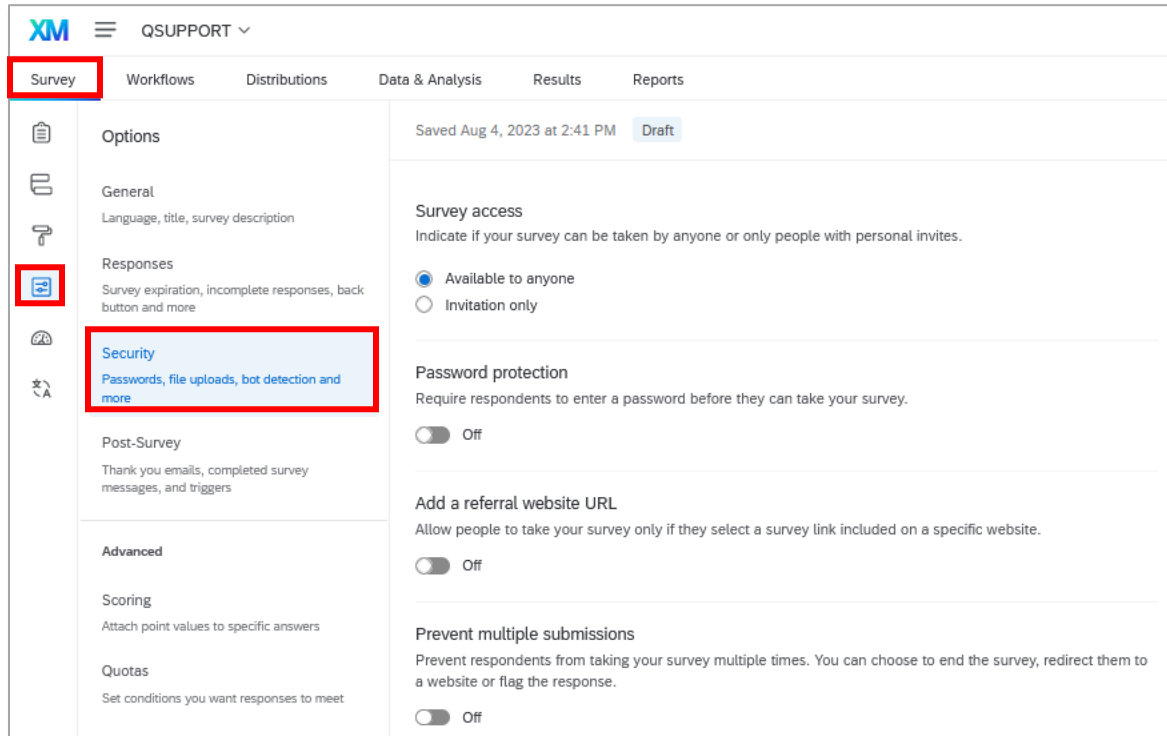
Examples of PII include, but are not limited to:

- Contact Information
- Student ID
- Date of Birth
- Parent Names
- Social Security Number
- Taxpayer Identification Number
- Driver's License Number
- Other unique identifier created or collected by government body
- Medical Information
- Grade/Employment Information

Find out more about Information Security Policies at <https://informationsecurity.wustl.edu/items/missouri-personally-identifiable-information-pii/>.

Where to access Security & Privacy Settings

1. Locate and select your survey to open the project
2. Select the Survey Options icon from the left side-bar menu
3. Select the Security option



The screenshot shows the XM Survey Options interface. The top navigation bar includes the XM logo, a menu icon, and the text "QSUPPORT". Below this is a horizontal menu with tabs: Survey, Workflows, Distributions, Data & Analysis, Results, and Reports. The "Survey" tab is selected and highlighted with a red box. On the left side, there is a vertical sidebar with icons for various survey options. The "Security" option is highlighted with a red box. The main content area displays the "Security" settings for a survey. At the top, it says "Saved Aug 4, 2023 at 2:41 PM" and "Draft". The "Survey access" section indicates that the survey can be taken by anyone or only people with personal invites. The "Available to anyone" option is selected. The "Password protection" section has a toggle switch set to "Off". The "Add a referral website URL" section also has a toggle switch set to "Off". The "Prevent multiple submissions" section has a toggle switch set to "Off".

Note: Security & Privacy settings are not retroactive. Only surveys delivered and responses collected after these settings have been saved will respond accordingly.

Privacy Setting Descriptions

1. **Survey Access:** Determine who can view / respond to a survey. To limit this access, select “Invitation Only”.
 - a. Available to anyone
 - b. Invitation only
2. **Password protection:** Require respondents to enter a password that has been assigned to the survey. To restrict access, select “On” and enter a password. Make sure to share the password with the respondents during survey distribution.
 - a. On / Off
3. **Prevent Multiple Submissions:** Prevent respondents from taking a survey multiple times. Whether or not to change the setting to “On” depends on whether the survey needs multiple responses for a single individual.
 - a. On / Off
4. **Bot Detection:** We’ll look for bots that might be taking your survey and flag their responses with an embedded data field (reCAPTCHA). It is best to change the setting to “On”.
 - a. On / Off
5. **Security Scan Monitor:** Prevent security scanners from accidentally starting surveys when they test your link (reCAPTCHA). It is best to change the setting to “On”.
 - a. On / Off
6. **Relevant ID:** Analyze a respondent’s browser, operating system, and location to prevent fraudulent responses. It is best to change the setting to “On”.
 - a. On / Off
7. **Prevent Indexing:** Block search engines from including your survey in their search results. This setting is “On” by default and should remain enabled.
 - a. On / Off
8. **Require Permission to View Uploaded Files:** This setting is targeted at collaborators on the project. If you wish to limit the number of people that can view uploaded documents within surveys, set this to “On.”
 - a. On / Off
9. **Anonymize Responses:** Don’t record respondents’ IP Address, location data, and contact info. Unless you plan to use IP Address, Location Data or other contact information, the recommendation is to set this option to “On” to enable anonymization.
 - a. On / Off

Privacy Setting Use Cases

Use Case 1: When requesting PII In the survey including the following data points:

- Name
- Address
- Email Address
- SSN
- Photos
- Video
- Audio Recording
- Telephone Number
- Birth Date (*recommend changing request to age*)

Use Case 2: When requesting PHI in the survey including the following data points:

- Name
- Address
- Email Address
- SSN
- Appointment Date
- Procedure Date
- Diagnosis
- Photos
- Video
- Audio Recording
- Telephone Number
- Birth Date (*recommend changing request to age*)

Use Case 3: When delivering surveys through platform tools, such as Prolific, Mturk or others used to obtain generalized data from large diverse participant populations, including the following data points:

- ID (*Prolific, Mturk, etc.*)
- Age
- Zip code
- Photos
- Video
- Audio recording

	PII	PHI	Platform Tools
Survey Access	Invitation Only	Invitation Only	Available to Anyone
Password Protection	On	On	Off (Unavailable using tools)
Prevent Multiple Submissions	On	On	On
Bot Detection	On	On	On
Security Scan Monitor	On	On	On
Relevant ID	On	On	On
Prevent Indexing	On	On	On
Require Permission to View Uploaded Files	On	On	On
Anonymize Responses	On	On	On