Sensitive Data

Download the PDF of this article.

In this Article

Related Articles

About Sensitive Data

If you are collecting sensitive data in your form, you can use FormAssembly's **Sensitive Data Feature** to indicate which specific fields contain that data. This is useful for compliance with the GDPR, HIPAA, or forms collecting payment information. Learn more about FormAssembly's security.

When you mark a field as sensitive, you can choose what type of data you are collecting:

- Credit Card Information (Credit Card Number and CVV Code)
- General Sensitive Data
- Password
- Personally Identifiable Information (PII)
- Protected Health Information (PHI) (available for Enterprise and Government plans)

If banking data, account numbers, passport numbers, and social security numbers are not marked as sensitive, this data will show in your responses.

Note: FormAssembly only stores sensitive data that is not credit card information. **Cardholder data is not stored on our servers**, and you must use a payment connector when collecting payment information so that cardholder data is processed securely through an approved payment gateway. Only the last 4 digits of a Credit

Card Number will be stored and viewable in the response data within FormAssembly, e.g., `xxxxxxxx1234`. CVV code data is never stored.

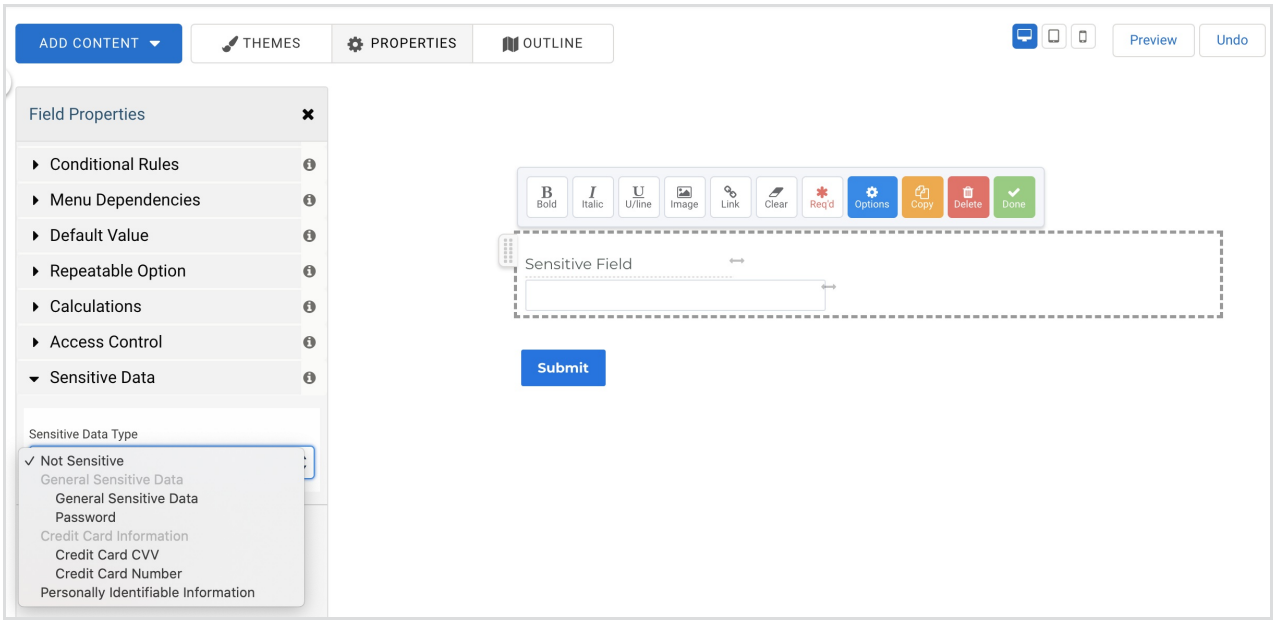
Note: When mapping fields marked as sensitive data in your connectors, the sensitive data will be sent as-is (unmasked), except for credit card information.

Note: When credit card and CVV code fields are added to a form and mapped into a payment connector, those fields will automatically appear as "sensitive" due to their connection with a payment connector.

Mark fields as Sensitive

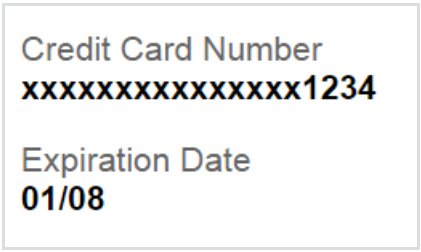
Add Sensitive Data settings in the Form Builder by completing the following steps:

1. Select the question that will be used to collect sensitive data.
2. Click on the **Options** button in the editing toolbar.
3. In the Field Properties sidebar, click the **Sensitive Data** section.
4. In the **Sensitive Data Type** drop-down menu, choose the option for your field.



You will see a flag on the Form Builder canvas labeled "Sensitive" next to any field marked as Sensitive:

Any cardholder data that is marked as Sensitive will be masked by default in your responses and in any connectors you may be using. All other types of sensitive data will not be masked on Basic, Essentials, and Team plans. Learn more about sensitive data management on Enterprise and Government plans.



Personally Identifiable Information (PII)

You can mark certain fields as collecting Personally Identifiable Information (PII).

PII is any information that can be used to identify an individual, such as a name, email address, social security number, or driver's license number.

Unlike credit card data fields, fields that are marked as containing PII will be saved in your responses as submitted. They will **not** be masked in the response data.

General Sensitive Data

There may be certain fields you wish to mark as containing sensitive data, even if they are not PII, PHI, or credit card information.

For any information you would like to mark as sensitive that does not fall into another category, you can use the "General Sensitive Data" category.

Unlike credit card data fields, fields that are marked as containing General Sensitive Data will be saved in your responses as submitted. They will **not** be masked in the response data.

Password Sensitive Data

Adding a password field will now automatically mark the field as sensitive. Passwords will be masked for respondents on the Review page. Learn more about enabling Review Before Submit.

Protected Health Information for Enterprise and Government Plans

You can mark certain fields as collecting Protected Health Information (PHI).

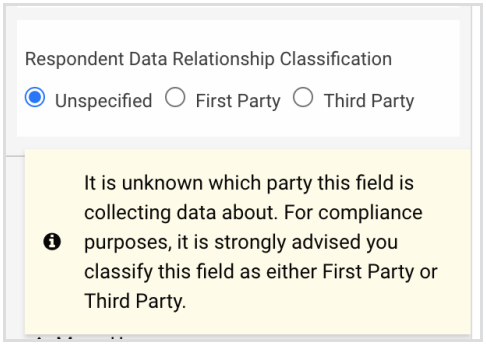
For Enterprise and Government plans, this feature enhances data governance and security. Administrators will now have control over which users can create and edit forms collecting specific types of sensitive data, and which users can view and edit responses with specific sensitive data types.

Respondent Data Relationship Classification

For every field marked as sensitive, you have the option to define the respondent data relationship classification.

In accordance with the GDPR, it's helpful to label the respondent data relationship. This will allow you to define if the person filling out the form is completing the form for themselves, for a third party person, or if it is unknown.

- **Unspecified:** It is unknown which party this field is collecting data about. For compliance purposes, you may classify this field as either First Party or Third Party.
- **First Party:** This field will be collecting data about the person filling out this form.
- **Third Party:** This field will be collecting data about someone other than the person filling out this form.



Using the Save and Resume Feature

If a user saves and resumes a form, the fields marked as "Credit Card Number" or "CVV Code" will be cleared. The previous information that the user entered into the field will no longer be available.

PII, PHI, and General Sensitive Data can be resumed with the stored values displaying, like other fields.

Form Moderation

All new FormAssembly forms on Basic, Professional, and Premier plans go through a moderation process to ensure they are collecting appropriate information that will be used ethically and legally.

By marking fields that collect credit card information or banking information as Sensitive Data, your form will help allow for a faster moderation experience, which will help get your form up and running as quickly as possible.

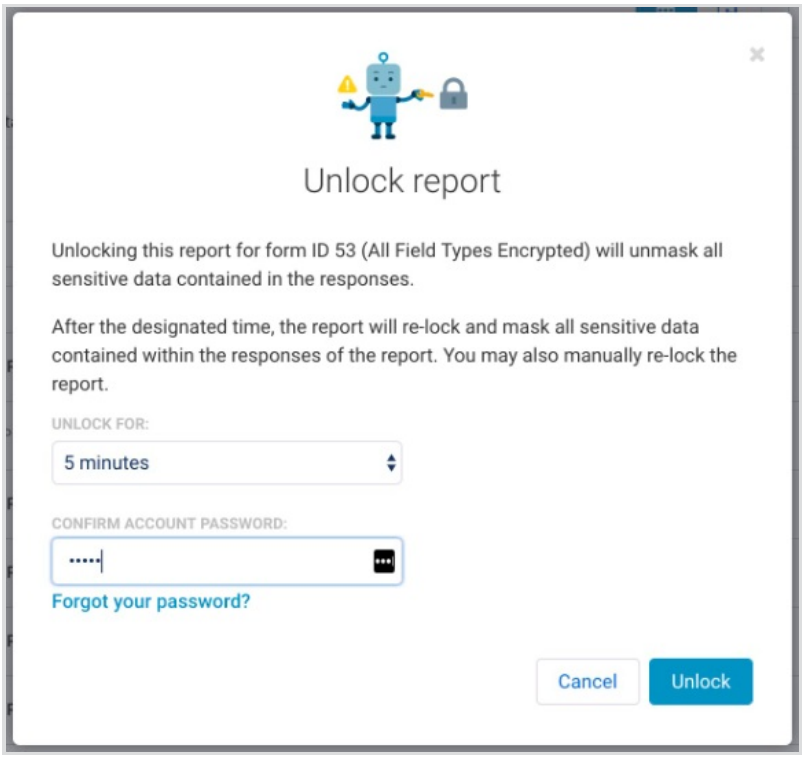
Sensitive Data Management on Enterprise and Government Plans

User Role Permissions

For enhanced data governance and security, Enterprise and Government administrators can manage, who can collect, or view and edit responses containing sensitive data. These controls are available through the Admin Dashboard. Learn more about managing user permissions.

Masked Reports and Responses

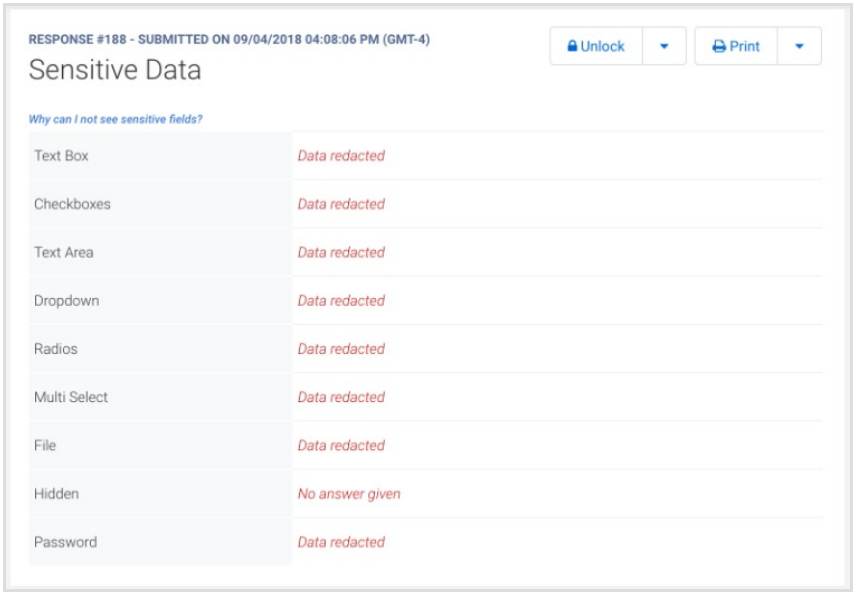
Sensitive data will be locked (masked) by default within responses and reports, and only accessible for specified lengths of time.



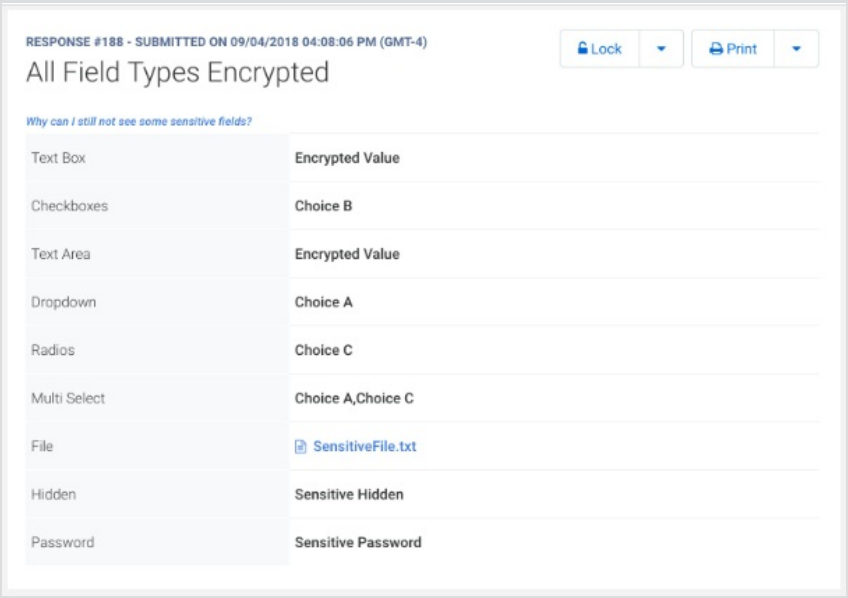
Sensitive data will also be secured and redacted in response aliases across Thank You pages, email notifications, and auto-responders. Individual field aliases, however, will pass sensitive data unmasked, so you can use them in calculations and formulas.

Note: Uploaded files are locked through the unlock/lock functionality on Enterprise and Government plans. They cannot be retrieved through the links listed in the responses until you unlock the responses.

Locked (Masked) Data:

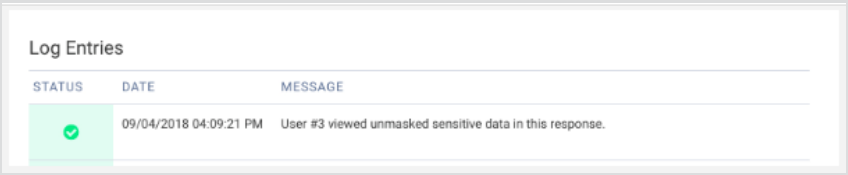


Unlocked Data:



Logging Access to Sensitive Data

When data has been unlocked, a log entry will show the date, time, and the person who unlocked and accessed the data.

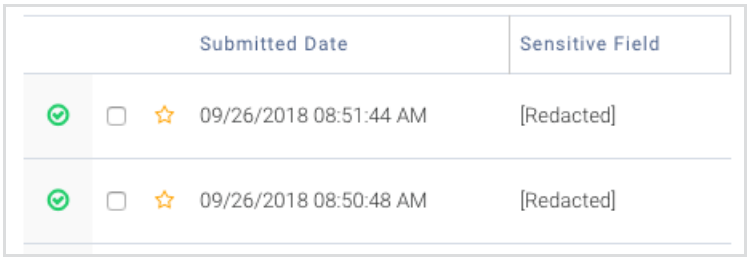


Unlock a Report

- Requires password (except for Single Sign-On)
- Requires permissions to view sensitive data
- Specify the unlocking time (will lock automatically after time expires)
- Unlocks the entire report (ALL responses for a form)
- If the form is shared, you cannot unlock the report for another user

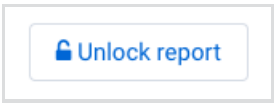
When you click on Responses, sensitive data is redacted for security. If your administrator grants you needed permissions to view sensitive data, you can unlock the report.

You will only be able to view the sensitive data types you can access. For example, if the form collects PII and PHI, but you only have access to view PII, the PHI data will remain masked when you unlock the report.

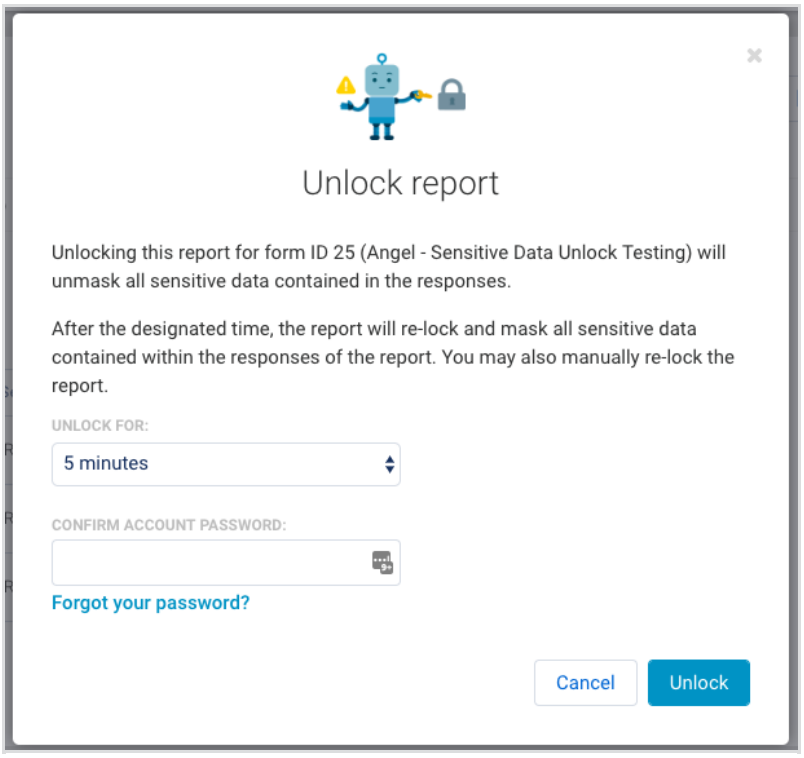


Walkthrough

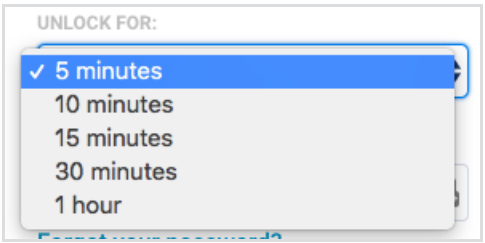
1. Click Responses
2. Click on Unlock report



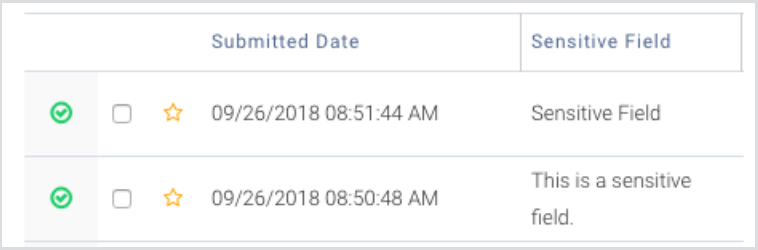
3. A pop-up box will appear so you can choose the amount of time you'd like the report unlocked.



4. Choose the amount of time you'd like to unlock the report.



5. Click Unlock



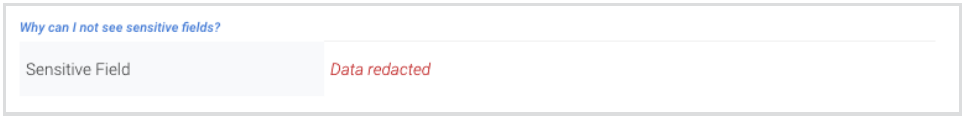
6. Once the time you have set for the report to be shown has expired, the field will be redacted once again when viewing the report.

Unlock a Response

- Requires password (except for Single Sign-On)
- Requires permissions to view sensitive data
- Specify the unlocking time (will lock automatically after time expires)
- Unlocks a single response, not the entire report
- If the form is shared, you cannot unlock the response for another user

When you click on Responses, sensitive data is redacted for security. If your administrator grants you needed permissions to view sensitive data, you can unlock the response.

You will only be able to view the sensitive data types you can access. For example, if the form collects PII and PHI, but you only have access to view PII, the PHI data will remain masked when you unlock the report.

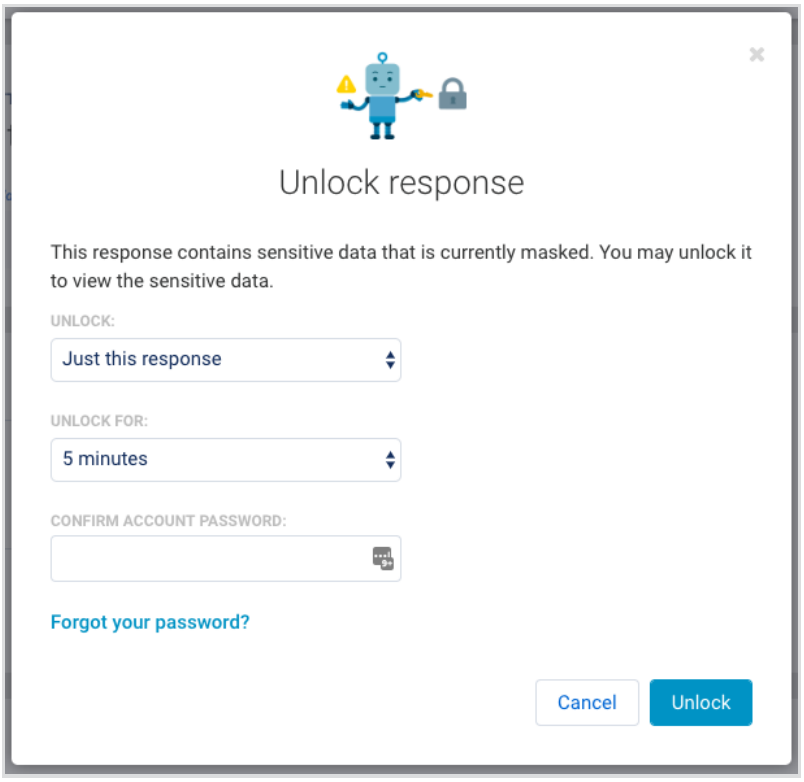


When you unlock and view a response, your access is recorded in the response Log Entries.

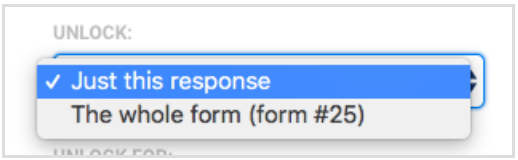
Walkthrough

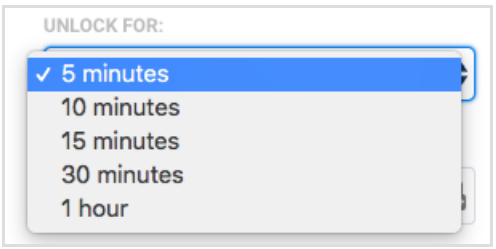
1. Click Responses
2. Click on the response you want to unlock
3. Click the Unlock button

4. A pop-up with options will show



5. To unlock just this response, choose Just this response from the Unlock dropdown. You can also unlock the whole form from here by choosing "The whole form".





6. After you have chosen the above options, you will then need to enter your password and click Unlock.
7. It will then show in your report as unlocked so you can view the data.

8. Once the time you have set for the data to be shown has expired, the field will be redacted once again.

Sensitive Data in Workflow Responses

Workflow Responses will follow the same sensitive data visibility permissions as the forms used in the Form Steps. This means that the form owner and administrators will be able to see all of the collected data (besides the standard masked password and credit card fields). Other users will only

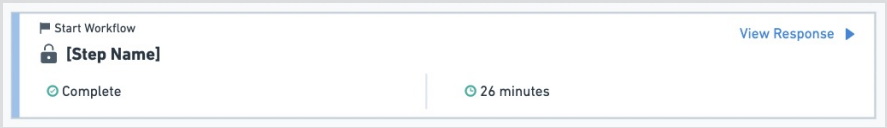
be able to view the response data that they have permission to view.

Team Plans

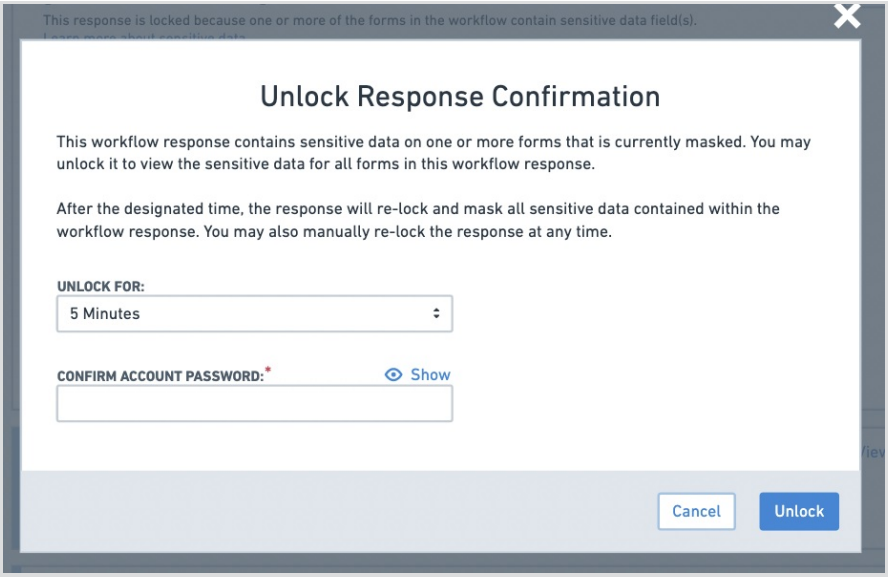
For Team users, PII and General Sensitive data will remain exposed in responses. Passwords and credit card data will be masked.

Enterprise Plans

When viewing response data as an Enterprise user, users will see each Response Card marked as "locked" if it contains sensitive data.



The Response Card can be unlocked by the form owner, administrators, and users with the correct permissions.



Once the response has been unlocked, permission-restricted sensitive data will be visible for the set amount of time. This means that if the user does not have the necessary permission to view PII, then data marked as PII will still be shown as "redacted" after unlocking the response card while other sensitive data that they do have permission to view will become visible. **This will not include credit card fields and password fields which will always remain masked.**