

@IP-ENCRYPT Action Tag

OVERVIEW:

Public surveys present an opportunity for fraudulent data. This is particularly true when compensation for participation is involved. In these circumstances, every possible measure should be implemented to prevent and evaluate fraudulent data. This may include several tools and methodologies (e.g., RECAPTCHA).

Identifying multiple submissions from a single IP address can “help” with fraud analysis. While there may be valid reasons for multiple submissions from a single IP address, it may also be an indicator of possible fraud. Combined with other analysis, the IP address could be quite helpful.

Because an IP address is considered a personal identifier, collection is generally avoided. However, it’s not the IP address that is most valuable. It’s knowing that multiple surveys were submitted from the same source.

Enter @IP-ENCRYPT, which captures an encrypted version of the IP address. This protects the survey submitter and also provides the ability for the study team to identify multiple submissions from the same.

When the @IP-ENCRYPT action tag is assigned to a TEXT field, an encrypted version of the IP address is captured to the field when the instrument is collected in Survey mode.

NOTES:

- The value is captured only upon the initial entry of the survey (if Save and Return is utilized from a different location at a later time, the encrypted IP address is NOT updated).
- If a proxy server and / or VPN client is being used, the IP address of that server captured.
- It is recommended that two additional action tags be applied: @READONLY and @HIDDEN-SURVEY.
- If necessary (and approved by IRB or the appropriate oversight committee), a REDCap administrator has the ability to decrypt a questionable IP address. This may provide additional helpful information.

IMPLEMENTATION:

1. Create a text field on the survey instrument.
2. Ensure that “Validation” is set to “---None---”.
3. Add the @IP-ENCRYPT action tag.
4. Recommended: Add the @READONLY and @HIDDEN-SURVEY action tags.

The screenshot shows the 'Add New Field' form in REDCap. The form is titled 'Add New Field' and includes a close button (X). Below the title, there is a paragraph of instructions: 'You may add a new project field to this data collection instrument by completing the fields below and clicking the Save button at the bottom. When you add a new field, it will be added to the form on this page. For an overview of the different field types available, you may view the [Field Types video \(4 min\)](#).' Below this, the 'Field Type' dropdown is set to 'Text Box (Short Text, Number, Date/Time, ...)' and is highlighted with a red box. The 'Field Label' section contains the text 'Encrypted Survey Taker IP Address' and a checkbox for 'Use the Rich Text Editor' which is unchecked. The 'Action Tags / Field Annotation (optional)' section contains the text '@HIDDEN-SURVEY @READONLY @IP-ENCRYPT' and is highlighted with a red box. The 'Variable Name' section contains the text 'encrypted_ip' and a checkbox for 'Enable auto naming of variable based upon its Field Label?' which is unchecked. The 'Validation?' dropdown is set to '--- None ---' and is highlighted with a red box. The 'Required?*' section has 'No' selected. The 'Identifier?' section has 'No' selected. The 'Custom Alignment' dropdown is set to 'Right / Vertical (RV)'. The 'Field Note (optional)' section is empty. At the bottom right, there are 'Save' and 'Cancel' buttons.