How to setup a REDCap Project for Compliance

We encourage the use of some/all of these features for a REDCap project as a part of good clinical practice, even if the project does not require 21 CFR Part 11 compliance (or IHC6 -GDPR). These features are designed for best practices for all projects.

This document is designed to help REDCap users understand how to configure REDCap to maximize compliance for clinical research studies. In order to do that, users should understand what each project setting/configuration is doing and how to properly enable each setting. Proper setup of each feature is required in order to mitigate risks associated with data integrity and regulatory compliance. While this is meant for project designers of REDCap, we realize there are many nuances in configuring REDCap, therefore we are adding REDCap Admin tips to aid the REDCap Admins.

Look for this icon 

To be fully compliant, both the REDCap instance must be compliant ready AND each individual project must be properly configured.

As noted above, it is considered best practice to implement the features described in this document for any study. However, to determine if they require a compliant system for their study, users should ask themselves the following questions:

1. Is my study regulated or subject to strict compliance?
    - Example: Clinical trials submitting data to the FDA.
2. Do I need a validated system or audit trail?
    - Example: Studies requiring proof of data integrity.
3. Does my study involve high-risk or sensitive data needing enhanced security?
    - Example: Multi-site regulated studies.

Quick Decision Rule:

- If yes to any of these: Users must use a compliant system
- If no: REDCap Production (i.e., standard VUMC REDCap instance) is likely sufficient.

Summary of Compliance Requirements

It is important to understand that compliance is not just about REDCap. REDCap contains functionality that allows you to apply settings required for compliance, but these in themselves will not make your project compliant. They must be applied within a framework of processes and documentation covering different levels; institutional, REDCap-specific, and project-specific. This is why we consider regulatory compliance applies at the study/project level, though all three levels are important.

Before we dive into the specific REDCap functionality, it is worth highlighting some of the institutional infrastructure you will need to have in place. These are standards that any organisation performing clinical research should have in place. Each element would probably require a document of explanation so be aware the following are for guidance only:

Institutional infrastructure

Institution-level infrastructure cover high-level issues that would generally apply across an organisation conducting clinical research including:

1. **System Validation:** Any system used to collect clinical trial data and documentation must be validated. You should be able to demonstrate the system functions in accordance with defined specifications.
2. **System Security**: Your system must be stored on servers configured to ensure your data are adequately secure. If your project is deemed not to require full compliance, it may be appropriate to store your data on a server managed locally. However, where a project will need to meet regulatory requirements, some institutions may choose to engage an external hosting provider such as Amazon Web Services or Microsoft Azure to provide more secure data storage. These providers offer a wide selection of hosting options such as mirroring of data across different physical locations and other infrastructure that is more sophisticated than many institutions would be able to support themselves. You need to consider:
    - Secure server location e.g. restricted/controlled access, controlled server environment and power supply.
    - infrastructure security mechanisms such as firewalls/encryption supported by ongoing security review and patching and change management of hardware and software.
    - data security e.g. data and files must be backed up regularly – ideally to several locations and at least daily – with disaster recovery exercises conducted periodically to show you can implement processes to retrieve data from backup files if a disaster should happen.
3. **Staff Recruitment and Training:** All staff should be suitably educated and qualified, with specific training provided where necessary to perform their role e.g. for systems and projects.
4. **Controlled documents:** All staff should be working to processes and procedures defined in standard operating procedures (SOPs). Policies and SOPs are classed as "controlled documents" so they should be managed within a document management system.
5. **Documentation:** You should have documentation covering all the above – system validation documentation, IT infrastructure documentation including records of security patching/maintenance and backup/disaster recoveries, staff CVs/training records including training to SOPs relevant to their roles/responsibilities, etc.

In addition to institution-level considerations, analogous project-level considerations would include validation of project applications, use of appropriate project-specific SOPs and training/documentation.

In short, your project must be supported by controlled processes and documentation that demonstrate adequate control over all aspects of the project. Even if your system is hosted by an external organisation, it is still your responsibility to obtain adequate documentation that demonstrates the information framework is fit for purpose.

REDCap System/Project level compliance settings

The main focus of this document is to describe how to apply the REDCap settings that should be implemented as part of an overall process to make your project compliant with regulatory requirements. The following section contains two parts, describing:

- how to apply specific settings in REDCap that are regulatory requirements. These may be at Control Center level and/or project level where appropriate
- how to implement REDCap functionality AND organisational practices in combination to meet regulatory requirements. Some functionality has to be used in specific ways (as described in SOPs) so simply applying settings is not sufficient.

Part 1 settings applied at the system level and/or the project level (and presented in the order in which they would appear in the Project Setup Additional Customizations functionality):

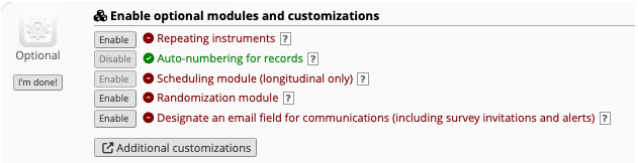
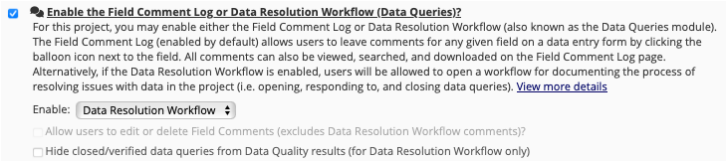
1. Data Resolution Workflow (DRW)
2. Record-Level Locking with PDF Confirmation
3. File Upload Settings
4. File Upload Field Enhancement
5. Logging (audit trail) Reason for change
6. e-Consent Framework

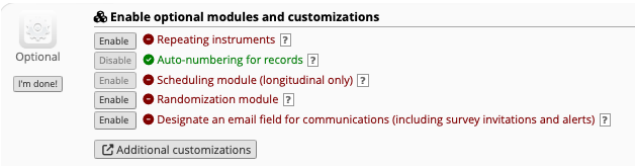
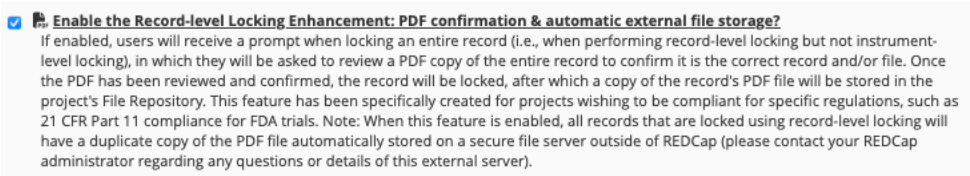
Part 2 settings that combine specific working practices with REDCap functionality settings:

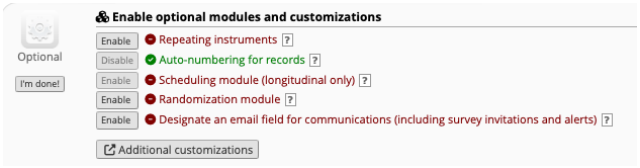
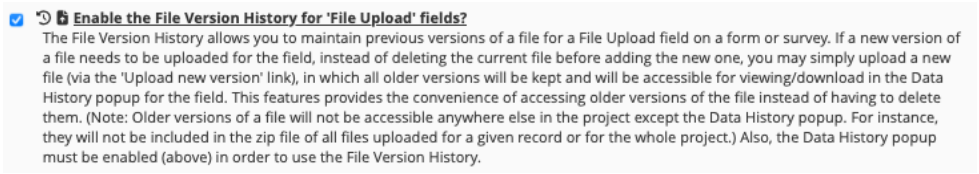
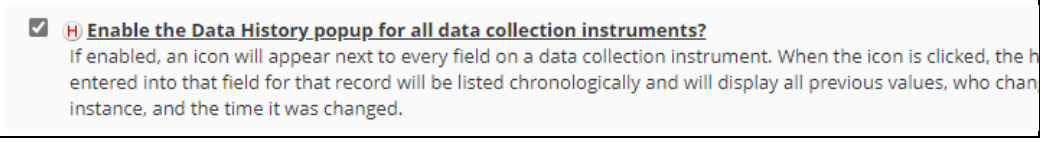
1. Uniqueness of username
2. User account management
3. Controlled user access to data and functionality
4. Password management
5. Electronic signatures
6. Device security
7. Project security using Status settings

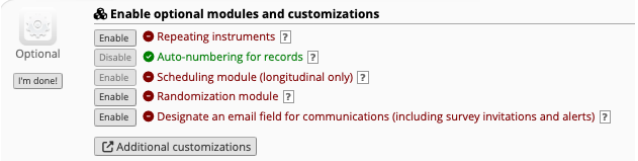
 If an option is not listed, contact the REDCap Administrator who must do additional configuration and they will need to review this document: Understanding Storage in REDCap

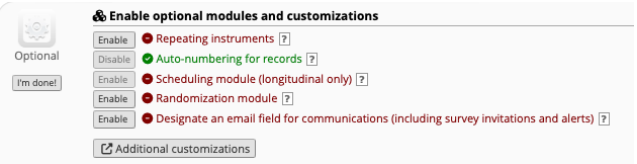
ADDITIONAL CUSTOMIZATION FEATURES (+ CONTROL CENTER where applicable)

Feature	Enable the Field Comment Log or Data Resolution Workflow (Data Queries).
Location	**Project Setup - Additional Customizations**
Description The data resolution workflow, often called 'data queries' in clinical trials and studies, can be utilized either on a data entry form (clicking the balloon icon next to the field) or on the Data Quality page when finding data discrepancies. For a brief overview, view the Data Resolution Workflow video. VIDEO: Data Resolution Workflow	**Why this is important** It is always important that we conduct project activities logically and consistently in such a way as to allow an inspector to follow the flow from start to finish. REDCap Logging provides an audit trail of the changes to data records, but it does not document the workflow that covers the data query process. This workflow would generally follow this sequence: • perform data quality checks (Sponsor) • review potential data issues (Sponsor) • raise queries related to unresolved data issues (Sponsor) • review and respond to data queries (Site) • review query responses and resolve or re-issue queries as appropriate (Sponsor) Traditionally, data queries were identified and documented on paper Data Clarification Forms (DCFs) that documented the query process and facilitated investigator review of the query and formal approval of corrections or other data changes. The Data Resolution Workflow allows this process to be managed within the REDCap infrastructure, which brings the benefit that the queries themselves can be managed centrally in real time with no risk of the query records getting lost in the post! **How to setup** On the Project setup tab, Click Additional customizations  Then check the option to Enable the Data Resolution Workflow feature and select from drop-down  **Note that this feature will also require the setup of data quality rules which are checks on data for completeness, logicality, consistency and appropriateness. These may be defined in a Data Validation Plan.** Defining rules to run in REDCap allows the DRW functionality to integrate checks, findings and queries. However, where data checks are more complex than the REDCap DQ rules can handle, they may be run external to REDCap and the queries manually entered into REDCap for subsequent management within the DRW. **Further information on using the DRW is appended to the end of this document.**

Feature	Enable the Record-level Locking Enhancement: PDF confirmation & automatic external file storage?
Location	Additional Customizations
Description The Record -level Locking Enhancement feature provides a secure backup copy of any locked form by creating a PDF and placing it on an external storage device. Generally, only the system administrator would have access to this file.	**Why this is important** 21 CFR Part 11 (11.10b) requires the "ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency." In addition to being able to create a human-readable copy of a record, it is important that the copy can be stored securely without risk of interference in order for it to be a reliable copy. You should be aware that files stored within REDCap (e.g. in the File Repository or File Upload fields) are not automatically encrypted and are also accessible for users to download and re-upload. Secure storage outside REDCap is therefore required to meet this requirement. This functionality is important because when a record is reviewed and locked, a PDF copy of the record (PDF) can be stored directly into an external storage repository. Since the repository may only be accessible to a system administrator, this backup of the record is considered sufficiently secure and therefore reliable. **How to setup** **In Control Center > Modules/Services Configuration** **In "Record-level Locking Enhancement: PDF confirmation & automatic external file storage" select setting from the first dropdown (e.g. Amazon S3, Microsoft Azure, etc.) and enter storage information as appropriate** **Then in the project:** **On the Project setup tab,** Click Additional Customizations  Then check the option to Enable the Record-level Locking Enhancement 

Feature	Enable the File Version History for 'File Upload' fields.
Location	Additional Customizations (note also includes “Enable the Data History Popup…”)
Description The File Version History allows users to maintain previous versions of a file for a File Upload field on a form or survey. If a new version of a file needs to be uploaded for the field, instead of deleting the current file before adding the new one, users may simply upload a new file (via the 'Upload new version' link), in which all older versions will be kept and will be accessible for viewing/download in the Data History popup for the field.	**Why this is important** Part 11 (11.10e) requires that “Record changes shall not obscure previously recorded information”. The REDCap Logging covers the data side of this requirement. REDCap also has the functionality to upload different versions of a file into the same File Upload field. Users clicking on the file link in the form will only see the current (i.e. most recently uploaded) version of the file. Any previous version of the file will not have been deleted but will be hidden on the main form. Functionality is therefore required to enable previous versions to be viewed. This feature is important in that it enables a user to view older versions of upload files via the field’s Data History popup (which must also be enabled and is also described below). Note: Older versions of a file will not be accessible anywhere else in the project except the Data History popup. For instance, they will not be included in the zip file of all files uploaded for a given record or for the whole project. Also, the Data History popup must be enabled (above) in order to use the File Version History. **How to setup** **In Control Center > Modules/Services Configuration** **Use the “Enable the File Version History for ‘File Upload’ fields?” dropdown to enable.** **Then in the project:** **On the Project setup tab,** Click Additional customizations  Then check the option to Enable the File Version History for File Upload fields?  **ALSO**, ensure the Data History popup functionality (also in Additional customizations) is enabled: 

Feature	Enable 'File Upload' field enhancement: Password verification & automatic external file storage.
Location	**Additional Customizations**
Description If enabled, users will receive a prompt when uploading a file for any File Upload field, in which they must confirm that they are uploading the correct file. They will also be asked to successfully re-enter their REDCap credentials as a verification step. (survey participants will not be asked to enter a password if on a survey).	**Why this is important** The action of uploading a file into REDCap carries a level of responsibility to ensure the file is correct before it is uploaded. File upload functionality is easy to use but in its raw form, does not implement any quality checks to verify the user has selected the correct file to upload. It is easy to click on the wrong file and be totally unaware of the error, so this is an area that carries increased risk. A check process must therefore be put in place to mitigate this risk. The 'File Upload' field enhancement functionality is therefore important for two reasons: • it forces the user to (check and) verify they are uploading the correct file before they perform the upload. This is done via a prompt for them to enter their password, similar to electronic signature functionality. • as noted in the setting above, files stored in REDCap are not subject to the same level of encryption and security as would be used to protect data. Using this enhanced functionality, a copy of the uploaded file will therefore also be sent to the external secure repository where it will usually only be accessible by a system administrator. The uploaded file will therefore be guaranteed to be reliable from the secure, external storage. **How to setup** **Control Center > Modules/Services Configuration** **In the "'File Upload' field enhancement: Password verification & automatic external file storage: section, select the setting you will use from the dropdown and nominate storage information as appropriate** **Then in the project:** **On the Project setup tab,** Click Additional customizations  Then check the option to Enable the File Version History for File Upload fields? Enable 'File Upload' field enhancement: Password verification & automatic external file storage? If enabled, users will receive a prompt when uploading a file for any File Upload field, in which they must confirm that they are uploading the correct file and will ask them to successfully re-enter their REDCap password as a verification step (survey participants will not be asked to enter a password if on a survey). This feature has been specifically created for projects wishing to be compliant for specific regulations, such as 21 CFR Part 11 compliance for FDA trials. Note: When this feature is enabled, all files uploaded via a File Upload field will have a duplicate copy of the file automatically stored on a secure file server outside of REDCap (please contact your REDCap administrator regarding any questions or details of this external server). Also, this feature does not work for Signature field types but only for File Upload fields.

Feature	Enable Require a 'reason' when making change to existing records
Location	**Additional Customizations**
Description If enabled, users will be prompted to enter a reason for changing the content of a record for any modification (including deletion) following the creation and initial saving of the record.	**Why this is important** Section 11.10(e) of Part 11 specifies the need for a computer-generated, time-stamped audit trail to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. REDCap logging functionality meets this requirement by default, so requires no setting to implement. However, recording reason for change for the audit trail is generally optional: • Part 11 does not specifically mandate the collection of a reason for change. • The newly-released ICH GCP E6(R3) Guideline section 4.2.2 (a)(ii) states:" Systems are designed to permit data changes in such a way that the initial data entry and any subsequent changes or deletions are documented, including, where appropriate, the reason for the change". • Likewise, section 6.2.1 of the European Medicines Agency (EMA) "Guideline of computerised systems and electronic data in clinical trials" states the need for recording reason for change in the audit trial to be "where applicable". Collection of reason for change is therefore an option that should be considered for appropriateness for a project. It is recommended as a means to document why a data change has taken place, though the burden on entry staff of storing a textual reason for change can sometimes mean the reason for change may still not be clear. **How to setup** On the Project setup tab, Click Additional customizations  Then check the option to Enable Require a 'reason' when making change to existing records ☐ Require a 'reason' when making changes to existing records? Require users to enter a reason (200 character max) in a text box when making any data changes to an already existing record on a data collection instrument. The prompt is triggered when clicking the Save button on the page. Any 'reasons' entered can then be viewed anytime afterward on the Logging page. Note: If the instrument does not yet have any data collected for it, then a reason will not be required (this includes importing data via the Data Import Tool). This feature is only triggered when adding, editing, or deleting data for an instrument that contains previously-collected data for one or more fields on the instrument.

Combined functionality and working practices

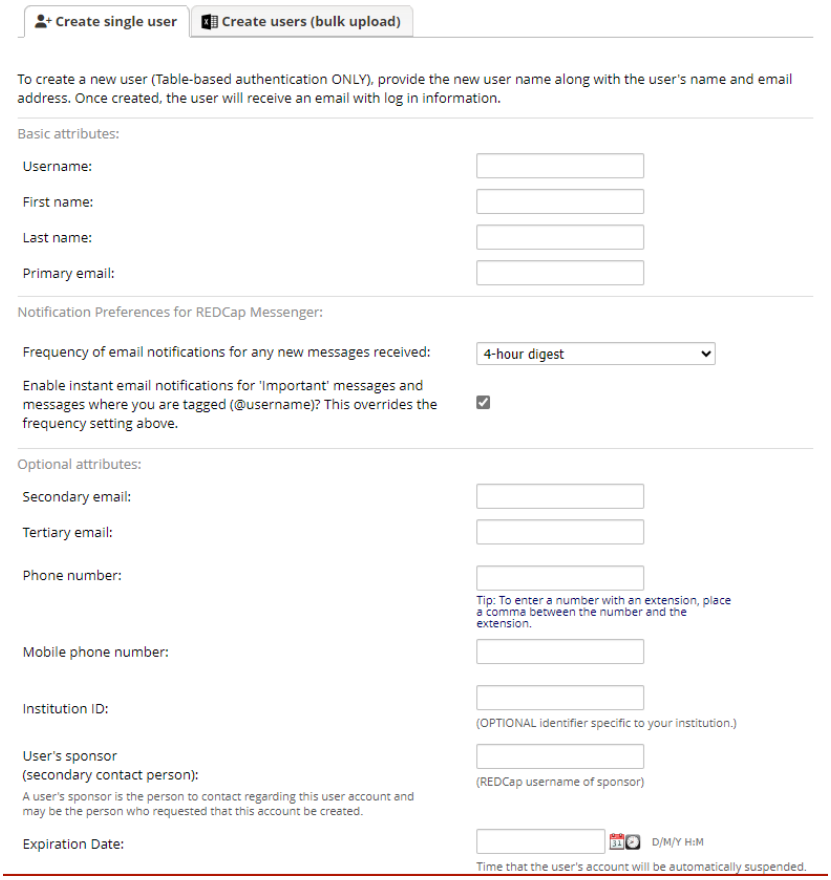
As noted above, some REDCap functionality needs to be used in specific ways in order to be compliant. The functionality should therefore be used in conjunction with specific working practices (e.g. SOPs) to which all users must be trained and have evidence of that training. The following are examples of this combined requirement:

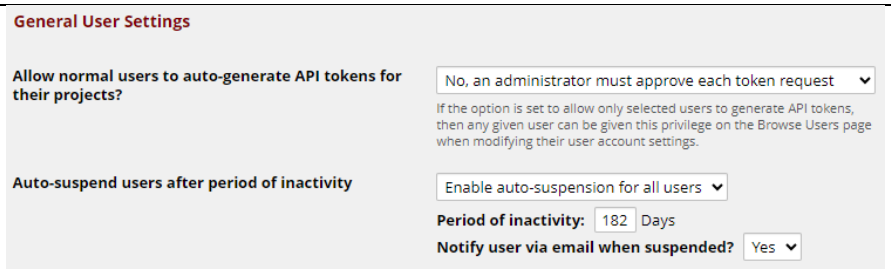
1. Uniqueness of username
2. User account management
3. Controlled user access to data and functionality
4. Password management
5. Electronic signatures
6. Device security
7. Project security using Status settings

Feature	**Uniqueness of username**
Implementation	**REDCap functionality + SOP/Working Practices**
Description All system users should be able to be identified uniquely.	**Why this is important** Section 11.10(d) of Part 11 requires limiting system access to authorized individuals. Similarly, 11.10(g) requires the use of "authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand" Both of these requirements require that we can uniquely identify every user of the system in order to ensure someone trying to access the system or a project is who they say they are. In other words, any user accessing the system should have an authorized, unique username and be using a password known only to them. Even if users at the same organisation have the same name, their system usernames should be different in order to manage each individual's access to the system. In addition to restricting users to access system, project, data and functionality, it is necessary to ensure that any action attributed to an individual's username in the audit trail can be reliable. It should not be possible for any individual to refute that an action attributed to them is false and we must be able to rely on the audit trail to be a perfect reflection of all recorded actions for the project. **REDCap Functionality** REDCap will prevent the allocation of a username for a new user when that username has already been recorded in the system. This system-wide functionality allows individuals to work on multiple projects and always be identifiable.

	To access REDCap, an individual must enter their username and password. Access to the system is not possible without both being provided and confirmed within REDCap as a valid combination. This ensures that a user accessing the system can be identified uniquely. Even if two users happen to use the same password, the unique usernames ensure they can always be distinguished. REDCap allows for a username to be deleted or suspended when an individual no longer requires access to the system. See below for why we should use suspension but should not use deletion of accounts. **SOP/Working Practice** **Individuals should be personally responsible for controlling their login information responsibly. Users should generally not share a username.** Given that REDCap enforces uniqueness of username, it should not be possible for a user to access REDCap on behalf of another user unless they actively share their confidential credential information. Working practices should define how individuals should manage their credentials responsibly, including keeping passwords confidential (i.e. no post-its round their monitor!) and not sharing details with others. **When an individual no longer requires access to the system, their username should be <u>suspended and not deleted or re-used.</u>** Throughout the system lifecycle (i.e. from commission to decommission), it should always be possible to identify all actions by an individual. It should be possible to continue to access this information even after they have left an organisation. Processes should ensure that administrators do not delete usernames or otherwise re-allocate a username to another individual at a later date; this would lead to uncertainty over the identity of who performed an action as recorded in the audit trail.

Feature	**User Account Management**
Implementation	**REDCap functionality +SOP/Working Practices**
Description In order to give system access to an individual, there must be a means to ensure their identity is verified, they are formally authorized to be given access to the system, and periodic checks are conducted to ensure they retain access or	**Why is this important** Section 11.10(i) requires that "persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks". In addition to requiring identification of individual users, Part 11 and GCP also require individuals to be suitably qualified to perform their role, and implicit in this requirement to verify an individual's identity. This is covered by a combination of Human Resources (HR) recruitment/onboarding practices that most institutions would be expected to have, along with project management procedures that use an individual's resume/CV to verify their qualifications and experience to perform their role.

are suspended according to need.	System administrators, or those allocating REDCap user access rights to an individual, may not know the individual in question, so there needs to be a request process involving an authorized requester (e.g. investigator) plus monitor review of CV/Signature and Delegation Log to verify the access request. Individuals may leave an organisation or otherwise no longer require access to a project. In case they do not notify the system administrator of this, periodic checks should be performed by suitable personnel to check on the currency of user access rights. **REDCap Functionality** REDCap functionality is limited in this particular regard, unless an organisation uses a REDCap database as part of its recruiting/onboarding processes. There is no dedicated REDCap functionality to manage access requests, though again, a REDCap application could be built to manage and authorise access requests. REDCap functionality can be used to automatically a suspend user account (a) after a specified period of time/on a specified date or (b) after a defined period of inactivity. These defaults should be considered to act as a catch-all in case other processes fail. This functionality can be found in: (a) Control Center > Add Users (Table-based Only) [Expiration Date field]  (b) Control Center > System Configuration > User Settings > General User Settings functionality.



SOP/Working Practice

Managing User Accounts

There are various responsibilities and processes that can cover this requirement.

An organisation's normal recruitment/onboarding procedures should verify an individual's identity while also verifying their qualifications and experience via collection of a resume/CV.

Structuring the access request process is highly recommended, though it is likely there are a variety of different approaches to managing this. It is particularly important for a clinical trial, where investigator site staff are likely to belong to a different organisation.

It is expected that all individuals at site should be authorised to perform specific tasks via completion of a Site Signature and Delegation Log. In addition, their training should be recorded in a Training Log and their resume/CV should be present in the Investigator Site File. The Principal Investigator may verify this as part of the request to REDCap admin, or the request may be approved by the study monitor before the request can be actioned by the REDCap administrators.

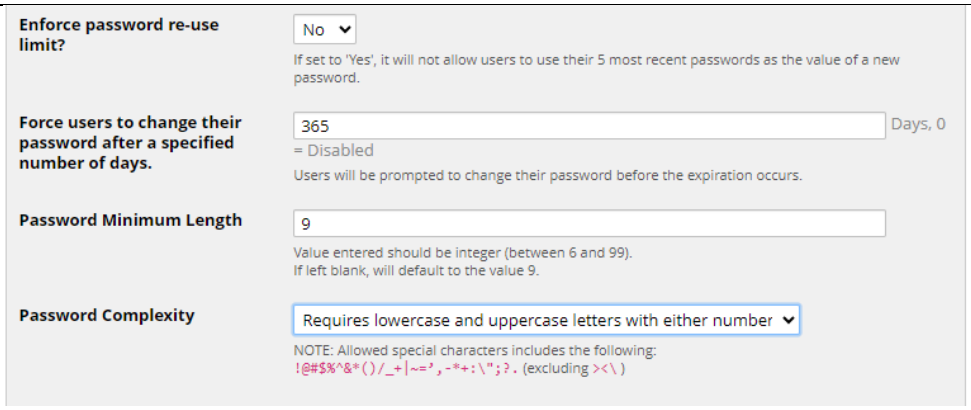
It is important to aim to keep the user access rights to a project "current". With an access request process in place, it is expected that new users will be added as required. However, it is more challenging to ensure the list of "current" users accounts for individuals who no longer require access. As noted above, REDCap offers functionality that will expire accounts according to date or lack of account activity. These can act as a catch-all that can be implemented during setup or whenever a new account is added.

[Not part of setup as such but for completeness] If an individual or their organisation notifies the sponsor organisation that access is no longer required, this makes the process easy. Since this does not always happen, there needs to be a proactive approach to reviewing access. This may use reports that are reviewed periodically, or monitors may ensure they review site access rights are current at their monitoring visits. These are two options, but others are likely to be used by other organisations.

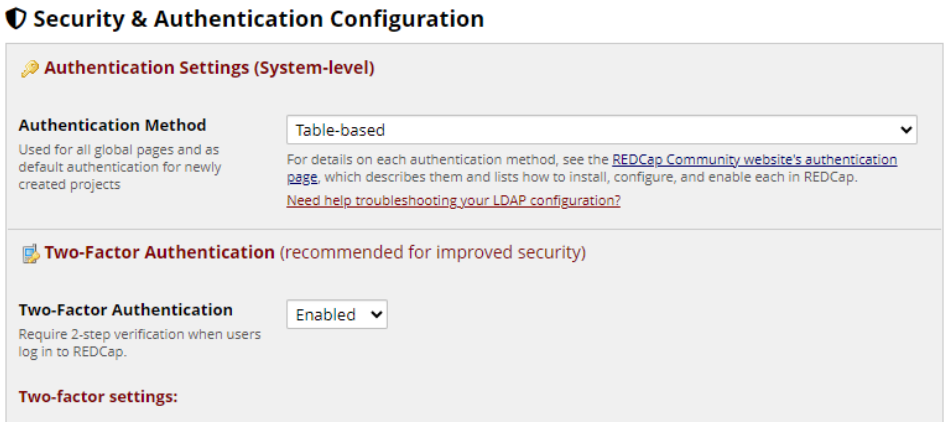
Feature	Controlled User Access to Data and Functionality
Implementation	**REDCap functionality + SOP/Working Practices**
Description System controls should be in place to ensure that any user can only access the project, data and functionality to which they are entitled by virtue of their designated role	**Why this is important** As noted above, section 11.10(g) requires the use of "authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand" The importance of username being unique in order to restrict access to the system to authorized individuals and ensure all actions performed by any individual are attributable was covered above. This section extends that oversight to the project level, covering accesses and rights granted to an individual for different projects. It is obviously undesirable that all users in the system have universal, unrestricted access to data and functionality; this would lead to breaches of confidentiality of the data and there would be no control over who could perform which actions. Part 11 therefore expects control of access rights down to the form/record level. To facilitate this, the system must provide a granular approach to granting user rights in order to provide maximum flexibility to control what any individual can do. **REDCap Functionality** REDCap User Rights functionality is designed to provide a high level of control over what individuals working within a project are able to see and do. In general, only system administrators should be able access any project without being granted specific access rights; all other users must be granted rights to access any project. REDCap User Rights offer control to: • grant/withhold access to a wide selection of basic privileges • assign levels of data viewing and export rights down to the form level • allocate a user to a Data Access Group (e.g. to restrict users at a site to accessing their site's data/records only)

	• configure External Modules. REDCap offers the functionality to assign users to "roles". This is an excellent way to define a standard set of rights to the role so that individual users assigned to the role will have the same rights as any other user assigned to that role. In some cases, it may be possible to use role-related Smart Variables to restrict users assigned to a role from accessing or not being able to access individual fields in a form. **SOP/Working Practice** **Managing User Rights** Managing the assignment of users to data and functionality access for a project will vary between institutions and projects and may be governed by institution- and/or project-specific working practices. The general approach should be to apply minimal rights where possible, restricting users to only the rights to which they are entitled. For a clinical trial scenario, it is important to distinguish between staff working at a "investigator site" level (i.e. participant-facing) and "sponsor" level (generally NOT participant-facing). Site staff should be assigned access to data based on their role (e.g. Investigator, Study Coordinator, Pharmacist, etc.) and limited to accessing their site's data. Sponsor staff may have access to data at all sites but there may be restrictions on which data they are allowed to see. To facilitate a consistent approach to management of user rights, the use of the REDCap "role" is encouraged. It may be helpful to devise institutional role templates that can be recycled from project to project.

Feature	**Password management**
Implementation	**REDCap functionality + SOP/Working Practices**
Description Passwords should be implemented and used in accordance with a Password Policy (or equivalent). Users must ensure their passwords meet strength requirements as defined in the Policy, must keep the password secure, and only use it as appropriate.	**Why this is important** Part 11 (11.200 and 11.300) references passwords in specific connection with the application of an electronic signature, however the use of passwords is also intimately connected with user login authentication (covered above) as well as verification of the correctness of an upload file (where that functionality is used). Passwords are the key piece of information that is personal to an individual and the security of their login credentials, so their use and security are paramount to retaining integrity of all user-directed processes. **REDCap Functionality** The REDCap Control Centre (REDCap Control Center > Security & Authentication Configuration) offers a variety of options related to password usage, including limits on password reuse, password expiration periods, minimum length and complexity of password content. Organisations will implement password management in their own way.



As a supplement to the use of a password, the increased use of multi-factor authentication can greatly enhance individual login security. It is an increasingly used feature in many systems and applications round the world today, whereby a code is sent to a separate device via an Authenticator app such as those offered by Google or Microsoft. REDCap administrators can enable the use of two-factor authentication at a system level, again via REDCap Control Center > Security & Authentication Configuration:

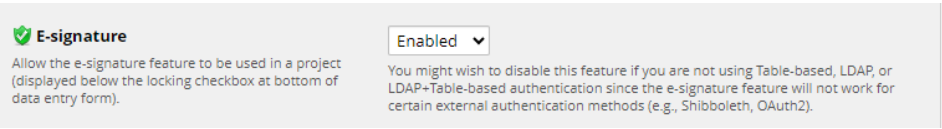


Further settings must be implemented further down that same form depending on the authenticator model and strategy used by the organisation.

SOP/Working Practice

Password Management

Passwords should be managed in accordance with a Password Policy that defines the organisation's requirements for strength, complexity, expiration, etc. combined with other considerations such as use of pass-phrase, password manager apps and two-factor authentication.

Feature	Electronic Signatures
Implementation	**REDCap functionality + SOP/Working Practices**
Description Electronic signatures are a central pillar of 21 CFR Part 11, since the Regulation centres round defining the way an electronic signature can be accepted as equivalent to a "wet-ink" signature on a paper document.	**Why this is important** Part 11 (11.50) defines the requirement for an electronic signature to have three components: 1. printed name of signer 2. date/time of signature execution, and 3. the meaning associated with the signature. These should be subject to the same controls as electronic records (e.g. covered by User Rights and audit trail) including inclusion as part of a human readable form of an electronic record. Part 11.70 takes this further by requiring that both electronic and handwritten signatures should remain linked to their respective electronic records in such a way that they "…cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.". Part 11.100 reiterates the situation that like login credentials, an electronic signature should be unique to an individual. Part 11.200 defines how system functionality for the application of electronic signatures should work, while 11.300 defines the need for controls to maintain security and integrity of electronic signatures, mainly relating to password security, some of which was covered above. It should be immediately apparent from the extent of the Part 11 referencing above that this is extremely important. From a functionality perspective, setup and implementation are defined in detail. The Regulation is also clear that a person applying an electronic signature should be aware that their electronic signature carries the same legal weight as a wet-ink signature. Misuse of credentials to falsify an electronic signature could lead to serious consequences. **REDCap Functionality** Electronic signature use needs to be set at the system level via the Modules/Services Configuration menu.  It should also be set at the project level via the "Customize & Manage Locking/E-signatures" link in the Applications menu, then by checking the appropriate box in the linked form:

Display the Lock option for this instrument?	Data Collection Instrument	Also display E-signature option on instrument?	Lock Record Custom Text
☑	Form 1	☐	Form 1 'Lock Instrument' Text
☑	Form 2	☐	Form 2 'Lock Instrument' Text
☑	Form 3	☑	Form 3 'Lock Instrument' Text

The electronic signature use is integrated with form locking, so the functionality will appear at the same time in the Form Status at the bottom of a form that is to be signed.

REDCap uses the user's login and system date-time to collect the first two elements of the electronic signature as defined above. See below for important note on E-signature meaning text.

SOP/Working Practice

Setting up Electronic Signature Meaning text

Important Note: Though REDCap is designed to collect "Lock Record Custom Text", it currently has no equivalent functionality to collect the electronic signature meaning.

Users must therefore devise a customised means to add the E-signature meaning to the electronic signature functionality in such a way as to ensure the meaning remains attached to the record (in form views, audit trail and all downloaded versions of the record) and is not subject to interference or other malpractice leading to falsification of the electronic signature. For example, an External Module may be devised.

It is recommended that electronic signature meaning should be agreed and approved at the project level, in order to minimise the chance that the text may need to be changed due to being unsatisfactory once deployed. It should be highlighted to be tested as part of the application validation testing prior to deployment.

Feature	**Device Security**
Implementation	**REDCap functionality + SOP/Working Practices**
Description There should be settings and practices focused on IT Security for device users. These could combine elements of participant privacy.	**Why this is important** Various sections of Part 11 deal with the need to ensure login credentials remain secure and we have covered the importance of username uniqueness and responsible password management above. However, there are other potential risks that require "common-sense" working practices to be implemented to help keep our login information secure. These relate to how individuals should follow good practice regarding use of their devices, to ensure they minimize the risk another individual could gain access to their credentials. We touched above on the scenario of post-in notes stuck round a monitor to remind a user of their login details and passwords. This is an obvious no-no. Other device-related security considerations might include: • try to ensure no-one watches you type in a password • lock a device, or log off, when not using the device

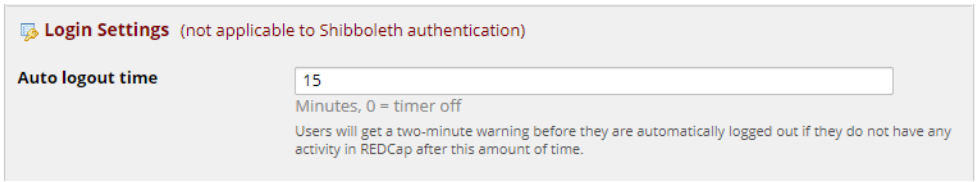
- use system settings to automatically lock a device after a period of inactivity
- use system settings to automatically lock an account after a period of inactivity or a number of failed login attempts
- if a device is lost or stolen, have procedures in place to minimize fallout
- try to avoid letting others see your monitor if you are looking at confidential information (more a privacy issue than specifically Part 11 but still good practice)

REDCap Functionality

In addition to the default functionality that password is not viewable on the screen while being typed in, REDCap has settings that can be implemented to lock accounts in different circumstances.

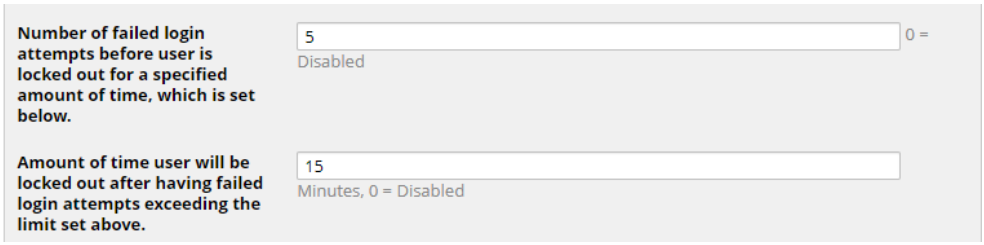
In Control Center > Security & Authentication Configuration

Set an Auto logout time after which an inactive device will log out



OR

Set a number of failed attempts after which an account will be locked, and for how long:



SOP/Working Practice

Good Practice when using a device

This information could be embedded in any number of SOPs such as those connected with maintaining participant privacy and/or good IT security practices.

Users should try to ensure that no-one can watch them type in their password when logging in. Of course, a professional colleague should not watch someone typing in their password, but trying to prevent someone seeing or guessing a password should always be considered.

In conjunction with REDCap system settings, devices should also be configured to lock after a period of inactivity, but both settings should be supporting the good practice of locking a device or shutting down when we stop using a device.

Ideally, devices should be managed centrally, so that in the event of a device such as a laptop being lost or stolen, an organisation has infrastructure to deactivate the device centrally following notification of the loss. In addition, a portable device should

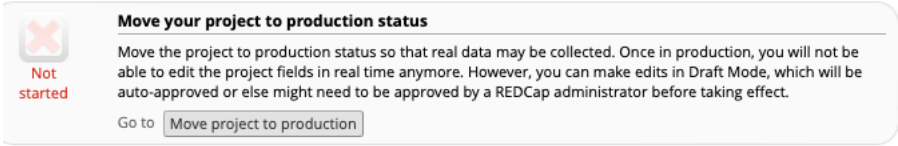
	be encrypted and from a privacy perspective, users should be discouraged from storing personal information of any kind on the device. Another privacy consideration is to be aware of who can see your monitor while you work. Users who deal with confidential information should try to ensure that no-one can read their monitor from behind them.

Feature	**Project Security using Status Settings: Move to Production.**
Location	**Project Setup page**
Description Move the project to production status so that real data may be collected. Once in production, users will not be able to edit the project fields in real time anymore. However, users can make edits in Draft Mode, which will be auto-approved or else might need to be approved by a REDCap administrator before taking effect.	**Why this is important** To maintain data accuracy and integrity, all REDCap projects should be moved to Production mode before real data is collected. There are several reasons for this: It is extremely easy to delete data in Development mode. This is by intent and is one of REDCap's handiest design and development features. However, this ease of deletion can be dangerous once real data is being collected, and so REDCap makes it considerably more difficult to delete data from projects in Production mode. (And it follows from this that test data should never be entered in a project in Production mode.) REDCap is pretty easy to use, but everybody makes mistakes. When REDCap projects are moved to Production a REDCap administrator must approve. This "proof reading" by the administrator frequently catches significant errors that the user has overlooked. Also, everybody occasionally forgets things. When this happens and a user modifies the design of a project to cover some issue(s) that originally was overlooked, there always is the chance that the change(s) will corrupt data in the project. For a project in Development mode that contains test data this is not an issue, however if the project in Development mode contains real data it can be a disaster. For projects in Production mode, all ex post facto changes are made in a parallel, "draft" copy of the project and not the actual project. The changes must be approved before overwriting the actual project, and if during the approval process REDCap detects that they may cause data corruption, the REDCap administrator is notified. REDCap is a very well-designed web-based data collection system and contains a number of safeguards. For projects in Production mode, REDCap can anticipate when data issues may arise and steers the user to a REDCap administrator for assistance in preventing accidental data loss and /or corruption. In Development mode, however, these safeguards are not in place. REDCap assumes all data in a Development mode project is test data and is unimportant and 100% dispensable in order to facilitate ease of design, development, and testing and puts minimum safeguards in the developer's path. The following project settings become locked down (unchangeable) to normal users for projects in production status. 1. All main project settings on the Project Setup page: Ability to enable/disable surveys, longitudinal data collection, and MyCap 2. Ability to enable/disable the record-autonumbering feature 3. Ability to enable/disable the Scheduling module (longitudinal projects only)

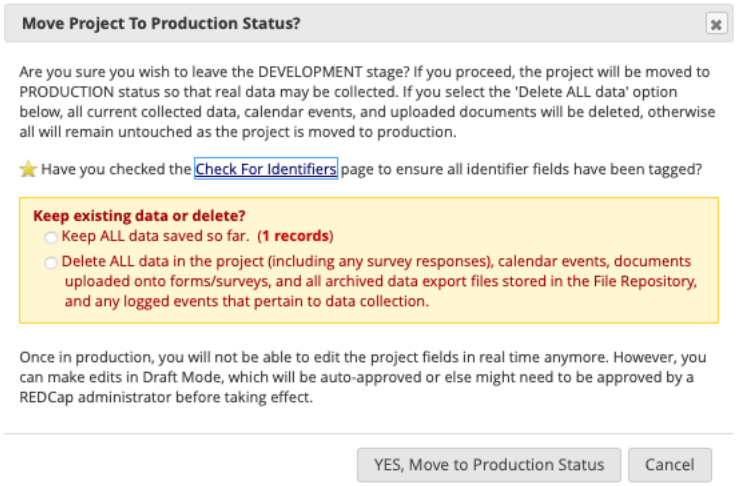
4. Ability to enable/disable the Randomization module
5. Ability to enable/disable the Twilio and Mosio telephony services
6. Ability to delete events
7. Ability to undesignate instruments from events to which they are already designated
8. Ability to disable the “Designate an email field for communications” feature if it is already enabled

How to setup

On the Project setup tab, Click the button labeled Move Project to production



Once the Move to Production button is clicked, users must then decide to keep or delete all the test data that has been placed in the project.



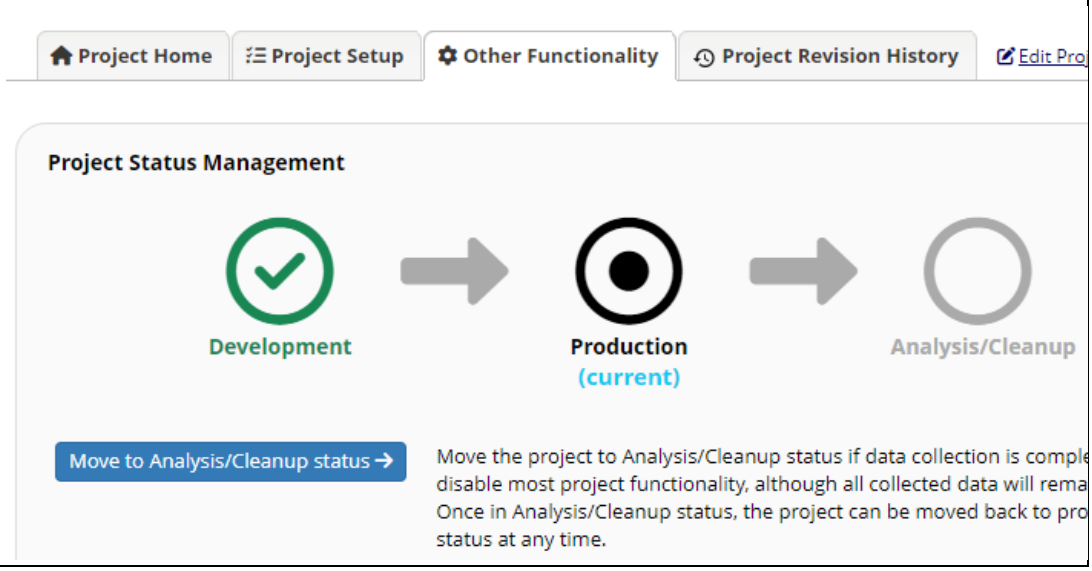
Click the YES, Move to Production button.

Depending on how REDCap has been implemented at a given site, it will either send a message automatically to the REDCap Admin to review the project or Automatically move it to production status.

For Compliance reason, the system should be configured to send an email to the REDCap Admin for review. This allows the Admin to review for errors in setup that could be found to be catastrophic in an audit.

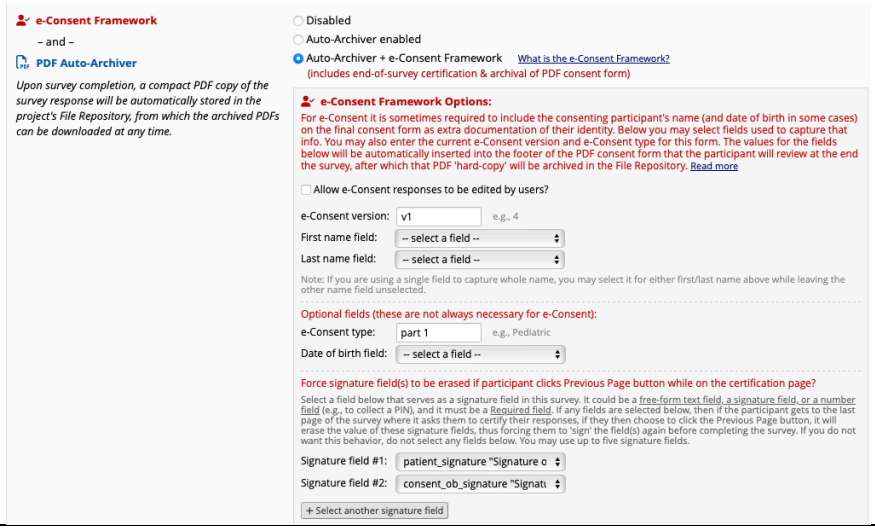
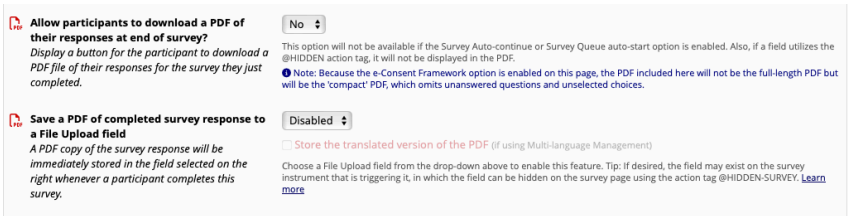
OTHER FUNCTIONALITY FEATURES

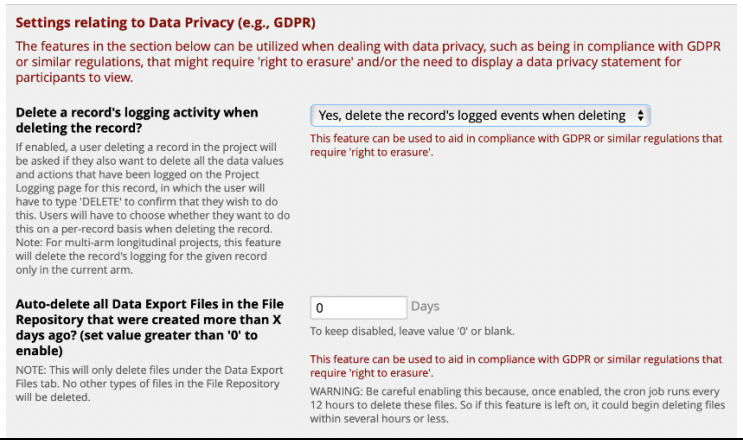
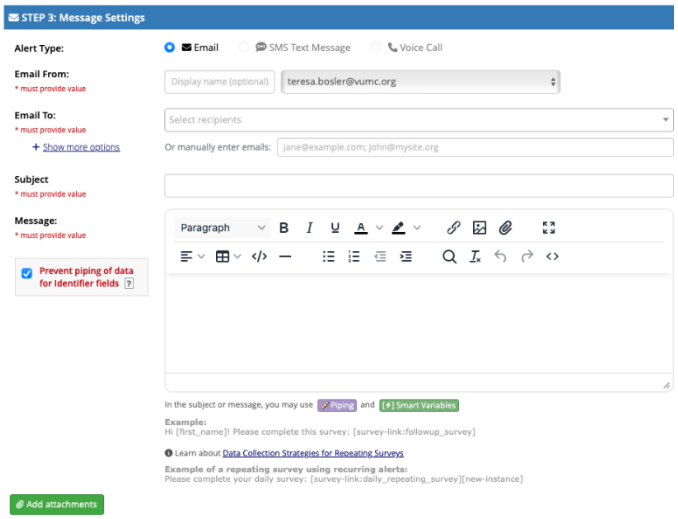
This feature is not strictly "setup" but for completeness it is useful to describe at this point.

Feature	Project Security using Status Settings: Move to Analysis/Cleanup status.
Location	Other Functionality
Description	**Why is this important** Move the project to Analysis/Cleanup status if data collection is complete. This will disable most project functionality, although all collected data will remain intact. Once in Analysis/Cleanup status, the project can be moved back to production status at any time. **How to setup** In the Project Setup > Other Functionality tab, press the button to "Move to Analysis/Cleanup status" 

EDIT PROJECT SETTING FEATURES

Feature	SETTINGS RELATED TO DATA PRIVACY (e.g. GDPR)
Location	**Edit Project Setting (only accessible by a REDCap Admin)** The features in the section below can be utilized when dealing with data privacy, such as being in compliance with GDPR or similar regulations, that might require 'right to erasure' and/or the need to display a data privacy statement for participants to view. Care should be exercised when dealing with data deletion and doing this accordance to the laws in your area.

Description	**Why is this important** The General Data Protection Regulation (GDPR) is a regulation regarding data protection and privacy in the European Union (EU), the European Economic Area (EEA), and the United Kingdom (UK). You can learn more about the GDPR on the System's GDPR website. REDCap, as a data collection tool, can be used to collect data subject to the GDPR. While GDPR applies across EU and UK, each country still retains its own Data Protection legislation, so it is still important to be aware of the national laws ON TOP OF the general GDPR legislation (e.g. France has a specific ban on the collection of Date of Birth). Any questions regarding how certain participant requests are handled should ALWAYS be directed to your institutional Ethics board/GDPR Office or Privacy Office. **How to setup**
Participants have the right to be informed about the collection and use of their personal data.	• Consent documentation and process. Consult your ethics board (IRB). • REDCap's eConsent module (in Survey settings) 
Participants have the right to view and request copies of their personal data.	Perhaps the best way to tackle this would be institutional, in conjunction with a site (since if GCP is being followed, except in special circumstances, a sponsor would not know who a participant is (pseudonymisation), so they could only provide a participant with a copy of all their personal data if the participant contacted the site and the site provided the sponsor (who hold the data) with the study ID/IDs, as the participant may have data held in more than one database. • The institution should have a policy or procedure regarding Right to Access • REDCap's email confirmation with PDF attached. • REDCap's Alerts and Notifications email with PDF. (in survey settings) 
Participants have the right to request inaccurate or outdated personal information to be	• Be aware that just because someone REQUESTS rectification, that doesn't mean a controller is obliged to change the information if the data are supplied from a verified source. A note of the request should be made (Change History or Data Resolution Workflow) but should the change not be made it should be documented why the change was not made.

updated or corrected.	• User rights allow for editable forms or surveys. (Upon request is optional). Include an automated email with copy of PDF for edited forms/fields.
Participants have the right to request their personal information to be deleted Guideline on computerised systems and electronic data in clinical trials	• Be aware that just because someone REQUESTS erasure, that doesn't mean a controller is obliged to delete if the data are supplied from a verified source. A note of the request should be made (Change History or Data Resolution Workflow) but should the erasure not be made it should be documented why the delete was not made. • Adding a "Please delete my data" checkbox on each page of a survey may help mitigate the data deletion requests • REDCap's Edit project settings. Before erasing a subject record, a REDCap admin must temporarily turn on the option to delete the record's logged event when deleting. This should be reset after the deletion and should be done with a REDCap Administrators help. 
Participants have the right to ask for their data to be transferred to another controller or to provide to them. The data must be provided in a machine-readable electronic format.	• Be advised not to send via email if possible • REDCap's email confirmation with PDF attached. • REDCap's Alerts and Notifications email with PDF. Green Add Attachment lower left) 
Participants have the right to request the restriction or suppression of their personal data.	• Be advised that an institution may need to ask your Ethics board about retaining the data already collected, when the participant consented. • Consent documentation and process. Consult your ethics board (IRB). • REDCap's eConsent module • Develop a single option (Radio/Dropdown) field indicating the record's consent status.

	
Participants have the right to object to the processing of their personal data.	• advised that an institution may need to ask your Ethics board about retaining the data already collected, when the participant consented. • Consent documentation and process. Consult your ethics board (IRB). • REDCap's eConsent module • Develop a single option (Radio/Dropdown) field indicating the record's consent status.
Participants have the right to object to decisions being made with their data solely based on automated decision-making or profiling.	• Be advised that an institution may need to ask your Ethics board about retaining the data already collected, when the participant consented. • Consent documentation and process. Consult your ethics board (IRB). • REDCap's eConsent module • Develop a single option (Radio/Dropdown) field indicating the record's consent status.
Data subjects have the right to withdraw previously given consent to process their personal data	• Develop a single option (Radio/Dropdown) field indicating the record's consent status.