

Implementing eConsent in REDCap

AND SIMILAR EDC SYSTEMS

Authors: Antony Colles, Claire West and Matt Hammond

Implementing eConsent in REDCap

Contents

Contents.....	1
1. About the authors.....	3
2. Introduction	3
What is eConsent?	3
Existing Guidance on eConsent.....	4
eConsent in Clinical Trials of Investigational Medicinal Products (CTIMPs)	4
eConsent in other studies (non-CTIMPs)	4
What are eSignatures and how should they be used?	5
eConsent in REDCap.....	5
What is REDCap?.....	6
Hosting REDCap	6
Overview of useful REDCap features for eConsent	6
When is REDCap suitable?	7
3. Gathering Requirements for Your eConsent System	8
Number and type of participants.....	8
Physical setting and method	9
Level of witnessing/ observation:	10
Implications of requirements.....	11
Importance of gathering (and keeping a handle on) requirements	11
Checklist before building your eConsent system.....	12
4. Implementing the different parts of an eConsent system.....	12
Component parts of an eConsent system.....	12
Conveying Information to the Participant	13
Documenting consent.....	14
Documenting patient consent	14
Documenting that the researcher witnessed the consent	15
Storing copies of the signed eConsent form and providing a copy to the participant	16
Monitoring Consent	16
5. Useful tools in REDCap for eConsent	17
The REDCap eConsent Framework	17

External Modules	18
Saving PDFs of eConsent forms:	19
Controlling the flow of your eConsent process	19
Improving appearance/usability	19
Monitoring	20
Alerts and Notifications	20
REDCap Reports	21
Audit Trail.....	21
6. Keeping Information Secure	23
Validating External Modules	24
Sending Documents Via Email	25
Sending eConsent form links via text/SMS	27
Database Encryption/Security	27
7. Example eConsent System Structures in REDCap	27
Site Localisation	27
Countersigning.....	29
Hybrid Paper and eConsent	29
8. General Considerations and known issues	30
New PIS versions/updates during study/maintenance	30
Re-sending consent form links.....	31
Preventing participants from consenting twice.....	31
9. Where to get help	32
REDCap community forums	32
UKCRC REDCap user group and Trialaborate.....	33
Online	33

1. About the authors

Antony Colles is a Senior Data Programmer at Norwich Clinical Trials Unit. He has extensive experience in the design and development of eCRF and eConsent systems in REDCap, including for CTIMPs. He has contributed to development of the REDCap core system and developed and published several REDCap external modules currently in use globally.

Claire West is a Senior Data Programmer at Norwich Clinical Trials Unit. She has extensive experience in the design and development of eCRF and eConsent systems in REDCap. She has a background in programming and bioinformatics, and is a member of the Norwich CTU Methodology Group and the REDCap Community Forum.

Matt Hammond is Deputy Director at Norwich Clinical Trials Unit, a UKCRC registered CTU in the East of England. He has over 15 years' experience in the design and delivery of clinical trials and chairs the Norwich CTU Methodology Group.

2. Introduction

What is eConsent?

eConsent permits potential research participants to be provided with the information they need to decide whether to take part in a research study or not, via a tablet, smartphone or other electronic device. It also enables that decision to be documented using electronic signatures. The advantages in adopting these methods were evident during the COVID-19 pandemic, during which eConsent, along with electronic Patient Reported Outcome Measures (ePROMs) enabled studies to continue recruiting in a way that would not otherwise have been possible.

There are two distinct phases in eConsent:

Informing and educating the participant

The first phase is the process of informing and educating the participant about the risks, benefits and other important information relating to the research. This "informing" phase in eConsent can include video, infographics, audio, web-pages, graphics, podcasts to convey information on the study. The advantages in this are that it can be highly configurable for the participant and include interactive elements aimed at improving participant comprehension. It can also include a Knowledge Review element in which an assessment of the participants understanding of this information can be undertaken, and if necessary, further supplementary information can be provided. In eConsent, the informing phase is often delivered using a study tablet, smartphone or the participant's own electronic device.

Documenting participant consent

The second phase of eConsent is associated with the documentation of consent. As with the Informing phase, this can be undertaken electronically through the use of an electronic consent form and electronic signature referred to as eSignatures.

Note that eConsent does not mean the same as Remote Consent. Remote Consent refers to the collection of consent away from the recruiting site. Remote consent can employ eConsent methods however it does not necessarily need to. Likewise, eConsent is not *always* undertaken remotely and eConsent can be used to facilitate the consent process both remotely and on-site.

Also note that there is no fixed model for eConsent; it can be entirely remote, be used to enhance / supplement traditional on-site consent or be something in between. It is also possible, and often recommended for trials to use a hybrid system where it is possible to both use eConsent and traditional models (e.g. paper based consent).

The most appropriate model to use should be determined by an assessment of the risks of the study, the trial design and the population you wish to consent.

Existing Guidance on eConsent

The Medicines and Healthcare products Regulatory Agency (MHRA) and Health Research Authority (HRA) released a joint statement on the use of eConsent in September 2018¹. This document was primarily produced for researchers looking to use eConsent in clinical trials of Investigational Medicinal Products however also covered the use of eConsent in other forms of research. The document provided legal and ethical requirements for seeking and documenting eConsent in studies conducted within the UK. It also provided classification and guidance on the use of eSignature.

eConsent in Clinical Trials of Investigational Medicinal Products (CTIMPs)

The use of eConsent in CTIMPs has stricter requirements than its use in other forms of research. After the information on the research has been given to the participant, but before consent can be documented, there must usually be a discussion in real time between the participant (or proxy consent giver) and the investigator (or delegated member of the recruiting site) so that the consent giver can discuss the research and ask questions. This two-way discussion can occur in person, virtually or over the telephone and can be used not only to provide information on the trial, but also to confirm the consent giver's identity. During this discussion the consent giver must be informed of the nature, significance, implications, and risks of the trial so that they can make an informed decision about whether to take part or not.

Following this discussion, consent can be captured electronically, however a copy (physical or electronic) of the completed consent form must be provided to the consent giver. This can be in the format of a non-editable pdf which can be sent via email to the consent giver. Further information on how consent should be documented for CTIMPs is detailed in the MHRA/HRA Joint statement on seeking consent by electronic methods¹.

eConsent in other studies (non-CTIMPs)

The process for non-CTIMPs is like that for CTIMPs other than it does not usually require the need for a two-way discussion between the participant (or proxy consent giver) and the investigator (or delegated member of the recruiting site).

It is however recommended that the process be risk assessed and if appropriate additional steps be included (such as the two-way discussion). The type of consent process used will depend on the following considerations:

- The nature and complexity of the research
- The risks, burden and benefits of the research
- Any potential ethical issues directly relating to the research.

¹ <https://www.hra.nhs.uk/documents/1588/hra-mhra-econsent-statement-sept-18.pdf>

When undertaking the risk assessment, you should also consider whether:

1. you can trust that the person signing the eConsent form is who they say they are
2. you can trust that the form has not been altered in any way
3. you can be sure of when the form was completed
4. you can demonstrate all the above if required by audit / inspection

What are eSignatures and how should they be used?

The use of electronic signatures, or eSignatures, in the UK is covered by the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019² and Amendment of The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016³.

eSignatures can include signatures that are:

- Tick-box plus declarations
- Typewritten
- Scanned
- An electronic representation of a handwritten signature
- A unique representation of characters
- A digital representation of characteristics, for example, fingerprint or retina scan
- A signature created by cryptographic means

There are also three categories of signature type:

1. Simple electronic signatures
These include a stylus or finger drawn signature, a typed name, a tick-box and declaration, a unique representation of characters and fingerprint scans
2. Advanced electronic signatures
These are uniquely linked to the signatory, are capable of identifying the signatory, allow the signatory to retain control, and are linked to data within the signature that can detect any changes made.
3. Qualified electronic signatures
These are an advanced electronic signature created by a qualified electronic signature creation device (software) which is legally equivalent to a handwritten signature.

Fortunately, in most cases when using eSignatures in clinical trials, a simple eSignature will suffice.

As with all clinical trial processes, it is recommended that the type and form of eSignature used should be determined following a risk assessment. Further information on the use of eSignatures in CTIMPs and non-CTIMPs is detailed in the MHRA/HRA Joint statement on seeking consent by electronic methods¹.

eConsent in REDCap

REDCap is a secure web application for building and managing online surveys and databases. It is available free of charge to non-profit organizations and is a popular solution for building electronic

² <https://www.legislation.gov.uk/uksi/2019/89/contents/made>

³ <https://www.legislation.gov.uk/uksi/2016/696/contents>

case report forms for academic research. In addition, its eConsent framework provides a robust platform for building an eConsent system.

There are, however, several steps and considerations needed to implement eConsent within REDCap, which first time users must take to ensure compliance with the current guidance.

What is REDCap?

REDCap can be used to build data collection systems for anything from questionnaire-based trials to CTIMPs. It is produced by Vanderbilt University in the US, who license it free of charge to academic and non-profit organisations around the world.

More information about REDCap, including how to join the “REDCap consortium” and obtain a license is available here:

<https://projectredcap.org/partners/join/>

Hosting REDCap

REDCap is a web application and a self-hosted product so you will need to find a server to host it before you can use it for data collection or eConsent.

Popular options are:

- A server provided by the IT department at your institution
- Cloud hosting services such as Amazon Web Services (AWS) or Microsoft Azure

Institutional IT departments have traditionally been the most popular option. However, for teams with a reasonable level of IT skill, cloud hosting is becoming increasingly popular. The REDCap developers have worked with both AWS and Azure to produce quick deployment options for REDCap, which has made this option even more accessible.

Details on the hosting requirements, which your IT department would need, are available here:









<https://projectredcap.org/software/requirements/>

The quick deployment options for Azure and AWS are available here:

- Azure <https://github.com/vanderbilt-redcap/redcap-azure>
- Amazon Web Services <https://aws.amazon.com/blogs/publicsector/quickly-deploy-a-production-ready-redcap-environment-on-aws/>

Overview of useful REDCap features for eConsent

There are lots of features of REDCap which are useful for an eConsent system, and help it meet regulatory requirements. Many of these will be discussed later in this document in more detail, but they can be summarised broadly as:

	Automated emails – a built in system to automatically send emails to participants or staff triggered by actions within the system	Section 0 Page 20
	Audit trail – all data entered and viewed is logged by the system and can be viewed by an auditor	Section 0 Page 21
	eConsent Framework – a framework to activate within REDCap to provide an end-of-survey certification step & archival of PDF to a consent form	Section 0 Page 17
	Automatically generated PDFs – generate PDFs of an online survey page which can be stored, downloaded, or emailed to participants or staff	Section 0 Page 19
	eSignatures – a built in field type in REDCap, that allows users to scribe their signature using a finger on a touchscreen device or using a mouse.	Section 0 Page 14
	Secure permission-based access control – the ability to view, add and edit data is controlled on many levels, on each form and can be configured by user or by specified roles. Data can also be tagged as identifiable to further control individual data access.	Section 6 Page 23
	External modules - individual packages of software that can extend REDCap's functionality, behaviour, and appearance. Free to use and develop.	Section 0 Page 18
	Active, responsive community – a large user base to both drive change, discuss issues and solutions with, and share code.	See external modules and getting help sections

Many of these features are also available in other EDC systems, and depending upon your eConsent system requirements, the availability and importance of these may help you decide which eConsent system solution is suitable for your trial. This makes gathering requirements for your eConsent system an important step.

When is REDCap suitable?

The first question to address if you are thinking of using REDCap for eConsent is: is it suitable for the types of trials you are running at your institution?



REDCap is suitable for **simple signatures** only
– not for advanced or qualified signatures



Of the three types of electronic signature, REDCap can be used to capture the first - a 'simple' electronic signature, consisting of a typewritten name, or electronic representation of a participant's written signature.

If your studies are higher risk and require more advanced or qualified electronic signatures, REDCap may not be suitable.

3. Gathering Requirements for Your eConsent System

Before you start building an eConsent system, it's important to work out exactly what it needs to do.

Different studies can have very different requirements for eConsent.

When gathering requirements for an eConsent system, there are 3 broad areas to consider:

Number and type of participants

- ☐ **Single** participant, or a **dyad** e.g. patient and carer)
- ☐ Consenting on participant **behalf** (e.g. capacity issue)
- ☐ **Re-consent** needed (e.g. regaining capacity, child reaching age of consent for themselves)

Physical setting and method:

- ☐ **Remote** or **in-person** or mix
- ☐ Tablet/**Mobile** phone or computer
- ☐ eConsent only, or **hybrid** eConsent and paper
- ☐ **Offline** eConsent

Level of witnessing/ observation:

- ☐ **Open** online recruitment
- ☐ '**Simple**' eConsent (participant signing only)
- ☐ **Researcher** witness and countersigning

This list is not exhaustive but is a good place to start.

Number and type of participants

Will your study be recruiting individual participants, or 'dyads' such as patient and carer, parent and child?

If recruiting a dyad, it's advisable to use a **single record** in REDCap with two consent forms, one for each member of the dyad. This way the wording of the consent form can be adjusted for each participant as appropriate, while keeping the data for both members of the dyad together in a single

record. This approach should work equally well for groups of three or four participants recruited together.

Might one person be consenting on behalf of another?

For example, a relative consenting for a participant who does not have capacity to give consent.

If consent will **always** be provided by a relative, then this does not add much complexity. However, you may want to give the option of patient **or** relative consenting. If this is the case, you will need a pre-consent form to record whether it is the participant or relative providing consent, and two versions of the eConsent form - one for the participant to fill in themselves, and one for the relative to complete - and logic to display one or the other depending on participant capacity.

Might re-consent be needed?

For example, if consent is initially provided by a relative, but the participant regains capacity during the study, or a child who entered a study under their parent's consent becomes old enough to consent themselves

As above, you will need two versions of the consent form, and branching logic to display one or other depending on the participant's age or capacity. However, you will need to bear in mind that this could change during the study, so the branching logic should be written so that it doesn't delete the data from a form that has already been completed. You may also want a report that lists any participants who entered the study as minors but are about to reach the age where they can consent, so that they can be contacted for re-consent.

Physical setting and method

Will consent be remote or in-person, or potentially both?

If remote eConsent is planned, it is important to ensure participants will have access to a suitable electronic device. You will also need to choose a method of sending the eConsent form link to the device. This is usually by email or SMS message. You'll need to get verbal consent from the participant to store their contact details in order to send them the link.

You will need method of establishing identity remotely, for example through a phone or video call.

What device will be used for eConsent?

For example, will participants be consenting using a tablet, mobile phone, or laptop computer, or perhaps a mixture of all three?

The main thing this will affect is what kind of signature field is used. REDCap has an e-signature field for capturing an approximation of the participants' handwritten signature. However, this works much better when used on a touchscreen device than on a computer with a mouse. Using a mouse or a trackpad can make it very difficult to write a signature accurately.

Will the study be using just eConsent, or a hybrid of eConsent and paper consent?

To avoid excluding participants with no access to electronic devices, studies will often want to offer a choice of paper or eConsent. This adds some complications to the set-up. For example, the consent date, and any optional items on the consent form will be recorded into the database as part of eConsent. However, if the participant completes the consent on paper, these optional items will

need to be recorded manually by the researcher on a separate form. If you want to create a report of consent dates, or all participants who chose 'Yes' for a particular optional consent item, there are now two fields to check for each.

Online or offline eConsent?

Normally, eConsent will be done online via an internet connected device. However, there may be circumstances where eConsent needs to be carried out where no internet connection is available.

The REDCap team have produced a mobile app for Android and iOS devices which allows researchers to carry out eConsent and data collection offline and then upload the data to REDCap when a connection is available. However, this is not a simple option. It introduces a lot of complexity and extra processes, and greater risk of data loss. For example:

- Data is stored on mobile devices, so is at greater risk of loss if the device is lost or damaged
- Conflicts can arise between data stored on the device and data in REDCap while the two are out of contact
- Data can be lost if the study definition in REDCap is changed before all users have uploaded their data from the mobile devices.

In addition, many of the useful REDCap eConsent features are **not available on the mobile app**, such as the eConsent Framework, external modules, email alerts, and so on.

Successfully using the mobile app in a study requires a well-trained team of researchers, good technical support and very clear processes for how the devices should be used.

There are some good resources available on the REDCap community forum on how to use the mobile app successfully, which cover these issues in more depth.

However, in our opinion the mobile app should only be used as a last resort if access to the internet is impossible.

[Level of witnessing/ observation:](#)

To what extent do you need your eConsent system to document that consent was witnessed by a researcher?

This is likely to vary depending on the type of study.

For example, some low risk, questionnaire-based studies may recruit entirely online, with participants consenting online without ever interacting with a researcher.

Other studies may recruit via clinics and need to document the participant's consent, but not necessarily the researcher witness.

At the other end of the scale, a high-risk CTIMP study would need to document that the researcher had confirmed the participant's identity and witnessed them sign the consent form.

Open online recruitment

If your study is recruiting entirely online, then extra effort is needed to convey information about study. For example videos, simplified online PIS, links to the study website.

You will also need to add steps to confirm eligibility and participant identity as part of process. For example, for eligibility, asking the participant to answer eligibility questions prior to consent, and only let them continue to consent if they indicate they are eligible. For identity, add a verification step to check that contact details are genuine and a uniqueness check to try and stop participants from signing up twice. It's worth noting that it will not be possible to guarantee these absolutely as they will be self-reported.

If you need to record that a researcher has witnessed the consent, you will need to add an extra form for this. Further details on this are provided in a later section.

Implications of requirements

The requirements gathered above will influence the following aspects of your eConsent system:

- The number of forms you need
- The branching logic used
- External modules used
- Consent monitoring process
- eSignature field types (e.g. typed or handwritten signature)
- What email alerts will be required
- How you will record consent date and optional consent items
- What device or platform will be used (e.g. tablet, phone or PC and web-based or mobile app)
- Time needed to build, document, test and train users on your system

Importance of gathering (and keeping a handle on) requirements

We've looked at some of the main requirements for an eConsent system and the main factors to consider.





An important thing to remember is how these requirements can combine together and how this can affect the amount of time and effort needed to build, test, maintain and train people to use the resulting system.

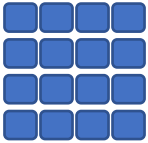


Each new option you add has the potential to **double** the number of processes, and thus the amount of time needed to build, test etc.



For example:

Requirements	Number of processes to document, build, test, maintain and train users on:	
Simple eConsent		1
eConsent + paper consent		2
eConsent + paper consent, remotely or in person		4
eConsent + paper consent, remotely or in person for a participant or consultee		8

eConsent + paper consent, remotely or in person for a participant or consultee with option to reconsent during study		16
...and so on	n	n

With a moderately complex project, what seems like just one additional request can have a disproportionate impact on the effort needed to build it. Study teams will often, quite understandably, want to build in the maximum amount of flexibility and different options for their participants to consent. However, there is a point at which the burden of building, training and maintaining the system outweighs the advantages of this flexibility.

Checklist before building your eConsent system

An example of things to ask to get to that list of requirements and know what to build in, and to give a rough timescale for teams:

- Will consent be just electronic, or on **paper** as well?
- Is this a **CTIMP**?
- Does consent need a **counter-signature** from a researcher?
- Will consent be done **remotely** (e.g. emailed/in person/both)?
- Does a carer or someone related to participant need consent (e.g. **dyad**)
- Will **internet access** always be available?
- Is it **open online** recruitment?
- Are there **multiple sites**?
- Is **monitoring** done centrally?
- Is the consent date or info in the consent form **used elsewhere**? (e.g. optional consent parts, or reports depending upon a single date)
- Will consent need to be taken **more than once**? (e.g. change of carer during study, child participant changes category)

4. Implementing the different parts of an eConsent system

Now we've looked at some of the differing requirements for an eConsent system, in this section, we'll discuss the core parts of the eConsent process, how you can implement these in REDCap.

Component parts of an eConsent system

Five parts of the eConsent process which can be performed electronically/within REDCap are:

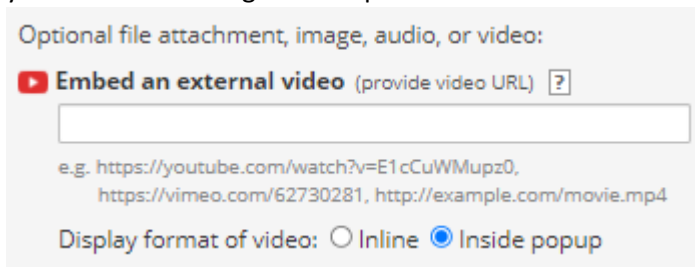
- Conveying information to the participant
- Documenting the participant's informed consent
- Documenting that the consent has been witnessed by a researcher
- Storing copies of the signed eConsent form and providing a copy to the participant
- Monitoring consent

We will briefly discuss each in turn in next five sections, and some guidance on what to consider when implementing them.

Conveying Information to the Participant

eConsent potentially offers more options for conveying information to a participant than paper consent. For example, it allows you to:

- link directly from the eConsent form to a website with more information about the study.
- embed a video explaining the study into the survey page before the eConsent form. In REDCap you can do this using a 'Descriptive Text' field:



Optional file attachment, image, audio, or video:

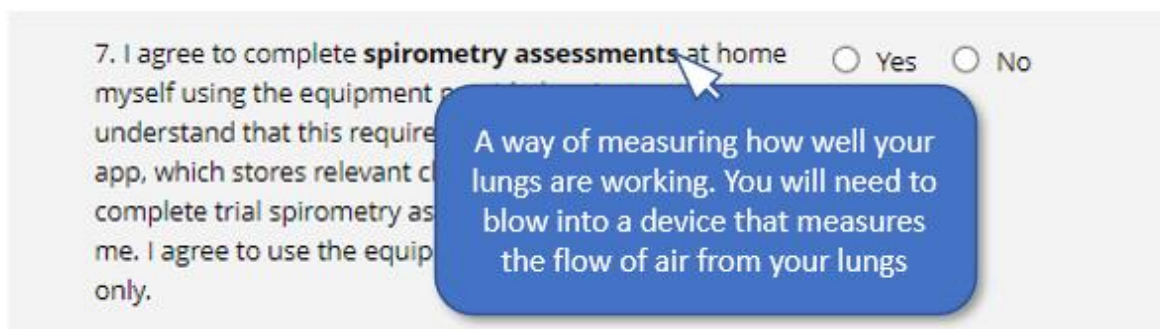
Embed an external video (provide video URL) [?](#)

e.g. <https://youtube.com/watch?v=E1cCuWMupz0>,
<https://vimeo.com/62730281>, <http://example.com/movie.mp4>

Display format of video: ☐ Inline ☒ Inside popup

Figure 1: Embedding a video into a REDCap descriptive text field

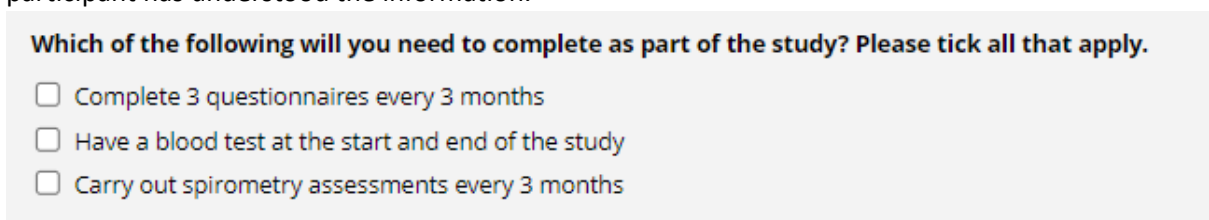
- add 'tooltips' with further information that can be displayed by holding a mouse over certain words on the page to help clarify unfamiliar terms. This can be achieved using the CSS Injector External Module in REDCap.



7. I agree to complete **spirometry assessments** at home ☐ Yes ☐ No
myself using the equipment provided. I understand that this requires a specific app, which stores relevant data on my phone. I agree to use the equipment only.

A way of measuring how well your lungs are working. You will need to blow into a device that measures the flow of air from your lungs

- Add a 'knowledge review' section. In REDCap you can add an extra questionnaire page between the Information Sheet and the eConsent form with a series of questions to ensure the participant has understood the information.



Which of the following will you need to complete as part of the study? Please tick all that apply.

☐ Complete 3 questionnaires every 3 months

☐ Have a blood test at the start and end of the study

☐ Carry out spirometry assessments every 3 months

Figure 2: An example of a knowledge review question

Another advantage of eConsent is that it can also increase the accessibility of the information to participant with differing needs.

- In REDCap you can enable Text-to-speech on any questionnaire and it will read out the questions to the participant.

Text-To-Speech functionality
(Allows text on survey page to be read audibly to participants.)



3. I give permission for my General Practitioner to be informed about my participation in the study.

- Providing the information in a web-page format enables participants to read it using their own accessibility devices, e.g. Braille monitors, screen readers and high contrast displays.

Documenting consent

Documenting patient consent

This can be done using an electronic version of your paper consent form, implemented as a REDCap **instrument** that has been enabled as a **survey**.

It typically has the following features:

- Header with logo identifying study
- Mandatory statements - these must be answered 'Yes' before the participant can consent.

1. I confirm that I have read and understand the participant information sheet dated 28.05.2021, version 2.4 for the above study and have had the opportunity to ask questions.


☒ Yes 

Figure 3: A mandatory consent item

- Optional Statements - the participant can answer either yes or no, but they cannot leave these blank

14. I wish to receive updates by email during my participation in the above study.



☐ Yes  ☒ No 

Figure 4: An optional consent item

- Record name/eSignature. This can be captured either as a typed name in a text field, or an approximation of a handwritten signature using the e-signature field type. The handwritten signature provides a slightly higher level of verifiability, but it can also introduce issues. If the participant is using a mouse, it can be very hard to produce a good approximation of your hand-written signature, which can lead to frustration for the participant, and rather undermines the point of using a handwritten signature in the first place. These are probably best used where consent can be taken using a touchscreen device like a tablet.

Name of Participant:

James Lind

Figure 5: A typed signature



Figure 6: a handwritten signature

- Consent date - this is a simple date field to record the date of consent. To reduce the chance of errors, make this field read-only using the @READONLY action tag, and automatically set it to the current date using the @TODAY Action tag.

Date:

10-05-2022 D-M-Y

How can I ensure that the participant completes all sections of the consent form before submitting?

Using Radio Button fields for all the consent items and making them **Required** means that the participant will see a warning message if they attempt to submit the form without completing all the sections. Additionally, using the **Auto Form Status** external module means that you can prevent the participant from even clicking the submit button until all the fields are complete.

Documenting that the researcher witnessed the consent

For many studies, especially CTIMP and higher risk studies, it is important to document that a researcher has confirmed the identity of the participant and witnessed their consent.

This should be implemented using a separate form with a name like 'Researcher witness' or 'Researcher countersigning'.

- It's a good idea to use either branching logic or the form **Render Skip logic** External module to ensure that this form only becomes available once the participant has signed the consent form. This avoids the risk of a researcher accidentally countersigning before the participant has consented.
- Using separate form creates a clean workflow and means that permissions can be set up so that only the Participant has access to complete the consent form, and only the researcher can edit the countersigning form.
- You can then use the **Multi-signature-consent** External module to combine both of these forms into a single PDF file to be filed and sent to the participant.

In a situation where the researcher witnessing the consent does not have a log-in to REDCap, you can enable the countersigning form as a survey and send a link to it to the researcher by email for them to complete that way.

Storing copies of the signed eConsent form and providing a copy to the participant

The guidance provided by the NIHR and MHRA requires the participant to be provided with a copy of their consent form. It may also be necessary for the sites in a multi-site study to keep a local copy of the signed consent form for all their participants.

This can be achieved by generating a PDF copy of the consent form.

REDCap eConsent Framework

The REDCap eConsent framework can be set to automatically provide the participant with a copy of the consent form to download immediately after completing it. However, this only works for a simple consent scenario where there is no researcher countersigning required. It is also of limited use if the participant is consenting in person on a device belonging to the clinic or hospital, as they will only be able to download to that device.

The eConsent framework also saves a copy of the consent form to the file repository. However, this is not always the most useful place to keep it. The file repository has very limited access control, with users either having full read/write access to all files at all sites, or nothing.

We would recommend using the following approach to storing PDF copies of the consent form:

Saving a copy of the form to a file upload field using Multi Signature consent EM.

Use the Multi Signature Consent External Module to save a PDF copy of the consent form (or combined consent and countersigning form) to a file upload field in the participant's record. This has the following advantages:

- Sites can be given read-only access to the consent forms for participants at that site only
- An email alert can be used to send the participant a copy of their consent form once it has been counter signed by the researcher.
- It can be easily integrated into a consent form review process

Monitoring Consent

One of the major advantages of eConsent is that it enables central monitoring of the consent process in real-time. This can be achieved in REDCap as follows:

1. Save a copy of the completed consent form to a file upload field, as described in the section above.
2. Set up an email alert to notify the monitor when a participant has consented.
3. Use the Image viewer External Module to display the consent form on the page for ease of viewing.
4. Add a field for the monitor to record when they have reviewed the consent form.
5. Create a report showing any outstanding unmonitored consent forms.

This creates an integrated monitoring system within the eConsent system, which enables the monitor to review consent at all sites without having to make site visits.

A similar approach can also be used for paper consent. The only difference is that the site staff would need to scan the paper consent form and upload the image file to REDCap instead of it being automatically generated.

It's also worth mentioning that the ability with eConsent to add real-time validation checks at the point of consent means there should be fewer errors in the consent forms in the first place. For example, common issues with paper consent forms are that participants have missed certain items, or not answered them correctly.

5. Useful tools in REDCap for eConsent

We've touched on some of the tools and features in REDCap that are useful for building an eConsent system. In the section we will look at these in more detail.

These are all things that have been useful to us in the past, but it's worth bearing in mind that every trial has its own requirements, and also new features are being added to REDCap all the time, so by the time you read this, better solutions may be available.

The REDCap eConsent Framework

This is what most people think of when they talk about eConsent in REDCap. It provides some useful functionality, but is not in itself a full eConsent solution. As the description of the feature in REDCap v 10.0.10 states:

[the eConsent framework is] referred to as a 'framework' because enabling this option alone does not provide an e-Consent process but merely provides the general framework or mechanism to allow you to provide e-Consent to patients/subjects

Additional features that it provides:

- End-of-survey certification & archival of PDF consent form
- Adds review, confirmation and download step to end of eConsent (see demo!)
- Version of ICF in footer of PDF

☒ **PDF Customizations**

Downloadable PDFs of data entry forms and surveys can be customized using the options below. Note: The options will be applied to ALL instruments in the project.

- 1) Set custom header text to appear at top left of every PDF page (it may be left blank, if desired). Note: Only static text can be entered; thus piping cannot be utilized here.
 Default text: Confidential
- 2) Display or hide the REDCap logo and website URL at the bottom right of every PDF page?
☒ Display REDCap logo and website URL (default)
☐ Hide REDCap logo/URL and instead display the following text: Powered by REDCap
- 3) Display or hide the Secondary Unique Field value at the top right corner of the PDF? (This option is only applicable if the Secondary Unique Field is enabled above and is set to be displayed.)
- 4) Hide Record ID from PDF header? (This will remove the record ID from the header of every PDF page.)

Figure 7: Setting for the REDCap eConsent framework

Pros of the eConsent framework:

- Settings are all in one place

- Quick start
- Well documented and tested
- Works well for simple consent on a laptop or computer.

Cons or things to be aware of:

- The consent form review step is nice, but
- some browsers don't display inline PDF files correctly
- Mobile compatibility issues – some mobile browsers will open the PDF in a separate tab, which can confuse the user and take them out of the consent workflow.
- Not suitable for use where the consent form needs to be countersigned by a researcher before giving the participant a copy
- Saves PDFs in the 'File repository', which has 'all or nothing' access control, so not appropriate for providing copies of the PDF to sites in a multi-site study.

External Modules





External modules are packages of code that add extra functionality to REDCap. They are typically developed by members of the REDCap community, and shared via a central repository, curated by the REDCap developers at Vanderbilt, rather like an 'App Store'.

There are over 200 of these modules available at the time of writing ([REDCap \(vanderbilt.edu\)](https://redcap.vanderbilt.edu/)) and they provide a huge boost to the functionality of REDCap. However, the quality varies, and you are responsible for thoroughly testing any module you download.

It's also worth mentioning that you can write your own modules for REDCap if you know how to program in PHP. You can either keep your modules for internal use, or share them with the community if you choose.

Here are twelve External Modules that we have found very useful for eConsent. We've categorised them into four areas of functionality:

- Saving PDFs of consent forms
- Controlling the flow of your eConsent process
- Improving appearance/usability
- eConsent Monitoring

 Saving PDFs of eConsent forms:	 Controlling the flow of your eConsent process	 Improving appearance/usability	 Monitoring
<ul style="list-style-type: none"> • Save PDF to field • Multi Signature Consent • Papertrail 	<ul style="list-style-type: none"> • Autocontinue logic • Form render skip logic • Auto Form Status * • HideSubmit 	<ul style="list-style-type: none"> • Survey UI Tweaks • Complete Row • CSS Injector • Javascript Injector 	<ul style="list-style-type: none"> • Image Viewer • showByRole

Saving PDFs of eConsent forms:

- Save PDF to field
 - Generates a PDF copy of a consent form (or any other survey) and saves it to a file upload field
- Multi Signature Consent
 - Similar to the above module, but with the ability to merge two separate forms into a single PDF
- Papertrail
 - Similar to multi signature consent, but with some additional options to customise the name of the resulting PDF, and run the PDF generation in the background so it doesn't delay the user in completing their surveys.

Controlling the flow of your eConsent process

- Autocontinue logic
 - Enables you to direct the participant to different survey forms depending on their answers. For example, if a participant indicates that they are not eligible for a study, they can be directed to an appropriate page.
- Form render skip logic
 - Like branching logic for forms. This module enables you to hide certain forms until certain conditions are met. For example, hiding a counter-signature form until the participant consent form is complete.
- Auto Form Status
 - Can be used to check how many blank questions are left on a form, and automatically mark the form as complete when all questions are answered. When used on surveys, it can be used to hide the 'submit' button until all questions have been answered. Useful for ensuring that a participant has answered all the consent items before they submit the form.
- HideSubmit
 - Can be used to hide the submit button on a survey until certain conditions are met.

Improving appearance/usability

- Survey UI Tweaks
 - Enables you to make changes to the appearance of a survey, for example changing the text on the 'next page' and 'submit' buttons, changing the width of the page, hide reset buttons etc.
- Complete Row
 - Automatically changes the colour of completed questions to clearly indicate which items are left to complete.

- CSS Injector
 - Can be used to add custom styling to any part of a survey or data entry form using CSS, for example to make the radio buttons larger and easier to click.
- JavaScript injector
 - Can be used to modify or add extra functionality and behaviour to surveys or data entry forms using JavaScript. For example, custom validation or specifying the type of keyboard displayed for a field on a mobile device.

Monitoring

- Image Viewer
 - This module allows you to display an uploaded image file on the page. This is useful for consent form monitoring, as the monitor can read the consent form on the page without having to download it. This saves time and increases data security. Currently works for PDF, JPEG, GIF and PNG files only
- showByRole
 - Allows you to show and hide individual fields based on the user's role. Useful for displaying a 'consent form reviewed' field that only the monitor can see and complete. Note, at the time of writing this only controls the appearance of the field on the data entry form, not in reports or downloads. It also can behave unpredictably when used on more than one form. We are in the process of submitting a fix for this issue to the developers.

Alerts and Notifications

REDCap's **Alerts and notifications** system can be used to send automated emails to members of the study team and to participants. It can also be set up to send SMS messages, although this requires the use of a third-party SMS provider.

Alerts can be triggered by an event in the database, for example a record being saved. They can also be triggered based on a date. For example, you can set an email to be sent to a participant six months after their date of consent.

Additionally, you can set criteria that must be met before an alert is sent, for example the consent form must be complete and countersigned.

Use cases:

- Sending eConsent form links to participants
- Sending copy of completed eConsent form to participant
- Alerting Study team that a consent form is ready to monitor

The alerts and notifications feature is built into REDCap with an easy to use interface.



Alert #2 Edit Options

If the following logic is TRUE when the instrument "PDF of eConsent form [Any Event]" is saved and has any form status: `[econsent_reviewed]='1' AND [econsent_pdf]!=''`

Send immediately

☒ Send one time (only once per record - i.e., never re-trigger)

Activity: 1 record was alerted ([view list](#)) Last sent: 03-05-2022 11:07

Email Preview

From: CHARMER Study <trialcommunications@uea.ac...>

To: [baseline_arm_1][cd_email]

Subject: Copy of your CHARMER consent form

Hi, Thanks for taking part in the CHARMER study. Plea...

Attachments (1):
[econsent_pdf]

Figure 8: An example of a REDCap email alert

REDCap Reports

REDCap has a built-in reporting tool which is useful for some aspects of consent. Reports are quick to build using a drag and drop interface. They can be viewed at any time via the REDCap web interface, giving you an up-to-date snapshot of the data, and can be easily exported in a range of formats including CSV, which can be viewed in Excel.

Consented but not randomised

Participant consented but abandoned baseline before randomisation

Record ID redcap_ id	Event Name redcap_ event_name	I agree to take part in the above study. cons_agree	Today's Date: consent_ date
165	Baseline	Agree (1)	28-11-2020
170	Baseline	Agree (1)	28-11-2020
171	Baseline	Agree (1)	28-11-2020
172	Baseline	Agree (1)	28-11-2020
180	Baseline	Agree (1)	29-11-2020
202	Baseline	Agree (1)	30-11-2020
205	Baseline	Agree (1)	01-12-2020
208	Baseline	Agree (1)	01-12-2020
211	Baseline	Agree (1)	01-12-2020
225	Baseline	Agree (1)	02-12-2020

Figure 9: An example of a REDCap report

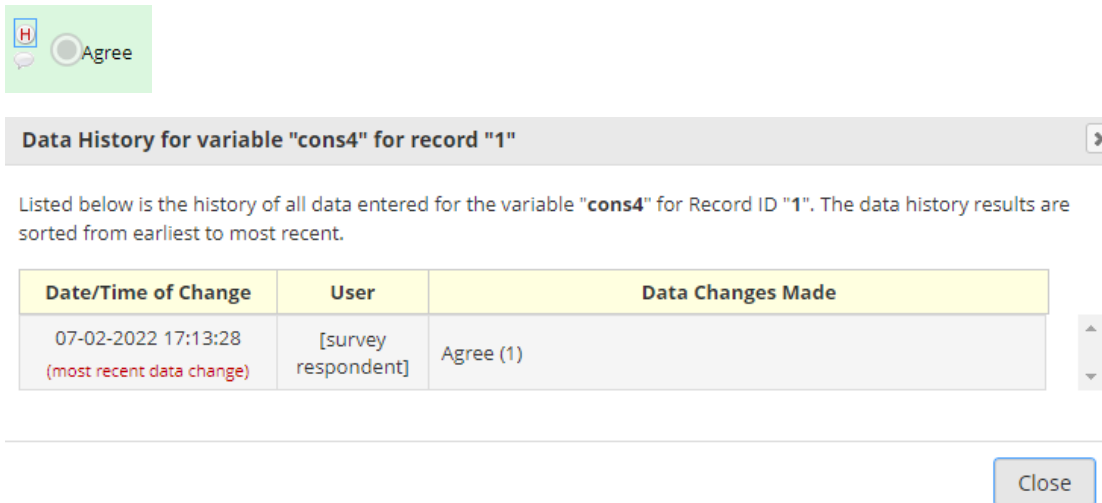
Examples of useful reports for eConsent are:

- Consent forms which are ready to monitor
- Participants consented and date, including site

Audit Trail

REDCap automatically logs all user and system activities in an audit trail. The time and date, the user who carried out the activity and which fields and values were affected are all recorded. It also records page views where no data were edited.

Changes to data can be viewed by clicking the **Data History** button next to the field.



Data History for variable "cons4" for record "1"

Listed below is the history of all data entered for the variable "**cons4**" for Record ID "1". The data history results are sorted from earliest to most recent.

Date/Time of Change	User	Data Changes Made
07-02-2022 17:13:28 (most recent data change)	[survey respondent]	Agree (1)

Close


Figure 10: The audit trail for a single field, viewed via the 'Data History Widget'

Data changes and all other activities can be viewed from the logging page. As a project administrator, you can control who has access to the logging page, so that this information is only displayed to users who need it.

e-consent feb 2022 test project

PID 345

Logging

 Export all loggi

This module lists all changes made to this project, including data exports, data changes, and the creation or deletion of use

Filter by event: Record created-updated-deleted

Filter by user name: All users

Filter by record: 7

Filter by time range from: to

Displaying events (by most recent): 1 - 4 (Page 1 of 1)

Time / Date	Username	Action	List of Data Changes OR Fields Exported
08-02-2022 12:13	[survey responde nt]	Updated Response 7	consent_form_complete = '2'
08-02-2022 12:13	[survey responde nt]	Updated Response 7	cons1 = '1', cons2 = '1', cons3 = '1', cons4 = '1', cons5 = '1', cons6 = '1', cons7 = '1', cons_emailyesno = '1', cons_email = 'a.colles@uea.ac.uk', first_name = 'Antony', last_name = 'Colles', signature = '22035', cons_date = '2022-02-08 12:12:21', consent_form_complete = '0'
08-02-2022 12:12	[survey responde nt]	Updated Response 7	elig_1 = '1', elig_2 = '1', elig_3 = '1', elig_calc = '3', eligibility_complete = '2'
08-02-2022 12:12	[survey responde nt]	Created Response 7	pis_notint = '1', record_id = '7', pis_complete = '2'

Figure 11: the audit trail, viewed via the logging page

6. Keeping Information Secure

A key requirement of any e-consent system is that it should store participant information securely, and only provide access to appropriate individuals.

REDCap offers a number of features to keep data secure:

Authentication

Access to the REDCap system is controlled using individual logins with a username and password. Passwords must be at least eight characters long and contain a mixture of numbers and letters. As a security measure, if a user attempts to log in with an incorrect password several times in a row, they will be automatically locked out for a period of time. The number of attempts and the duration of the lockout period can both be set by the administrator.

Alternatively, you can connect REDCap to your institution's user authentication system via Shibboleth, or use a mix of both these methods.

For extra security, REDCap provides options for two-factor authentication to confirm the identity of the user. This can be done via email, SMS text message, or using other authentication services.

Authorisation

Users can be given Permissions by adding them to a role. You could create a 'Researcher' or 'eConsent reviewer' role that has access to the eConsent forms, and add to this role only the members of the study team that are involved in eConsent. Other roles, for instance Statisticians, would not be given access to the eConsent data.

	No Access	Read Only	View & Edit	Edit survey responses
Clinician Contact Details	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Clinician eConsent Form (survey)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Researcher sign-off	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	
PDF of eConsent form	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	

Figure 12: setting instrument-level permissions for a user

Tag fields as identifiers

Fields in a redcap project containing identifiers such as names, addresses etc. can be tagged as identifiers. This can be used to exclude that data from exports, so that, for example, it doesn't get inadvertently included in an analysis dataset.

Identifier? ☐ No ☒ Yes
Does the field contain identifying information (e.g., name, SSN, address)?

Validating External Modules

External modules are shared by members of the REDCap community with no guarantees. The REDCap developers carry out a basic check for security issues before adding them to the repository, but it is important that you thoroughly test any modules your use in your projects.

Module developers often release new versions of external modules containing new features and improvements, which REDCap admins can download. It's important that you re-test the modules after downloading any updates, as these can sometimes break or alter existing functionality.

Do you need to do own validation
on External modules? Yes!



For each
project



At upgrade of
REDCap,
Module and
PHP version.
All can break
functionality.



Suggest
upgrading
modules and
REDCap at
same time to
reduce work



Have a plan to
work through
for testing all
functions.



Document
results of
testing

We recommend that you run a separate test instance of REDCap, and test updated modules before updating them on your live system.

We'd also recommend downloading and validating new versions of external modules at the same time as validating and updating your version of REDCap.

It's a good idea to write a validation plan, detailing the tests you will carry out to validate each module. If you write this in the form of a template, you can fill it out as you test, and this will serve as documentation of the validation process. It's also sensible to carry out a full re-test of a few projects, especially any that are high risk or feature multiple external modules. This kind of 'integration testing' will pick up if there are any issues caused by the modules working together.

[Sending Documents Via Email](#)

Sending documents such as signed consent forms by email is a slightly controversial topic. Some consider standard, unencrypted email to be insufficiently secure for this purpose.

Standard email is sent in plain text, unencrypted over the internet, and is thus potentially vulnerable to being intercepted via methods such as email server impersonation or planting malware in routers. However, this requires a high degree of technical skill and effort.

On a day-to-day basis, the main causes of email data breaches are:

- poor email security by the recipient- i.e. using a weak password on their email account
- user error during sending- i.e. the email is sent to the wrong recipient

The first of these is beyond our control as researchers. If a participant has agreed to receive a copy of their consent form by email, it's their responsibility to keep their email appropriately secure.

However, there are several steps we can take to tackle the second issue, and ensure that the email is sent to the correct address. These differ depending on the scenario:

[Remote consent](#)

If the participant is consenting remotely, and you are sending them the link to the consent form by email, this adds a built-in confirmation step to ensure that you have the correct email address. If they receive the link, then you know that the email address is correct.

In-person consent

This is riskier, as there is no built-in email verification step.

Require the user to enter, or at least check their own email address

We suggest that you design the process so that the participant enters their own email address, or at least has the opportunity to confirm or correct it before sending the signed consent form. This reduces a risk of a transcription error on the part of the researcher leading to an incorrect email address being used.

Add an email confirmation step

Alternatively, or in addition to the above approach, you should add an email verification step.

- Once the participant has entered their email address and saved the form, an email is sent to their address with a link to a 'confirm address' survey.
- This is a simple REDCap survey with a checkbox question saying, "I confirm that my email address is correct".
- The participant follows this link and submits the confirmation survey before REDCap sends them their signed eConsent form.
- This reduces the risk of the signed consent form being sent to an incorrect email address.
- It's still *possible* that someone else could receive the confirmation email in error and click the link, but this would be unlikely.

Alternatives to sending signed consent form by email

There is a more secure alternative to sending the signed consent form by email, and that is to build your own secure download system in REDCap.

1. Create a unique password for the participant at the point of consent. Save this in their record in REDCap and give it to them in person. Alternatively, ask the participant to create their own password and enter it as part of the consent process.
2. Use the multi-signature or Paper Trail EM to save the signed consent form to a file upload field. Ensure this field is on an instrument that is enabled as a survey.
3. Use the survey login feature to control access to the survey, so that it requires a user to enter the password to view it.
4. Once the consent form is countersigned, automatically send the participant a link to the survey. When they click the link, they will need to enter the password in order to download the consent form.

This adds complexity to the process - the user must remember and enter their password correctly or they will be unable to download the form. However, there is always a trade-off between security and convenience. It's a matter of deciding what is appropriate for your study.

Print the eConsent form and hand or post it to the participant

A relatively low-tech solution, as long as a printer available, although it does introduce an extra manual step.

Sending eConsent form links via text/SMS

It is possible to send a link to a REDCap eConsent form by SMS text message. To do this, you will need to create an account with an SMS service provider.

The provider that is easiest to integrate with REDCap is Twilio. Once you create a Twilio account and enable the Twilio features in your REDCap project, you will be able to send SMS messages containing survey invitations.

Occasionally, ethics panels and funders have raised data security questions about the use of Twilio as an SMS provider, given that it is a US-based company. We've looked into this in some detail and taken the following position:

1. Twilio are well aware of GDPR requirements, and explain at length the steps they have taken to meet them on their website.
2. No participant **clinical** data will be stored on servers in the US.
3. REDCap automatically erases the content of any messages sent via Twilio from the Twilio logs as soon as they are sent, leaving only a record of the time, date and phone number that the message was sent to.

Database Encryption/Security

During our webinar series, a few people asked whether eConsent data and copies of signed consent forms are encrypted on the server.

REDCap itself does not encrypt any data. Encryption must be implemented as part of the hosting for your REDCap install

- It is strongly recommended that you set up a security certificate on your server to enable encrypted connections using https, as this encrypts and protects data in transit over the web. This is standard security practise for almost any website.
- It is also strongly recommended to encrypt and protect with a password or PIN any mobile devices that you use for the eConsent process. This feature is enabled by default on most modern Android or iOS devices.
- It is also possible to set up your server to encrypt data at rest. Azure and AWS offer this as standard.

7. Example eConsent System Structures in REDCap

As mentioned previously, REDCap is a very flexible system, and there is usually more than one way of achieving something. However, we have included below some examples of how we have set up some common eConsent functions.

Site Localisation

If a study requires the eConsent form to be localised with details such as the logo of the NHS trust for the site, this can be achieved using Descriptive Text fields and Data Access group based branching logic.

- Create localised form headers using a separate descriptive field for each site. Include the logo and/ or names and contact details as necessary

- Add branching logic to the descriptive field causing it to be displayed only if the record is in a certain Data Access Group.


Learn how to use [Smart Variables](#) [Piping](#) [@ Action Tags](#) [Field](#)

[Return to list of instruments](#) [Survey settings](#)

Current instrument: **e-consent** [Preview i](#)


[Add Field](#) [Add Matrix of Fields](#)

Variable: `hdr_nnuh` Branching logic: `[record-dag-name]='01_norwich'` [How to embed a field](#)



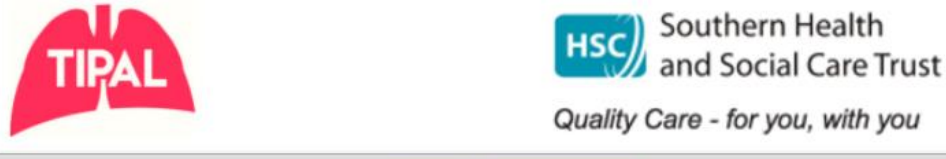
[Add Field](#) [Add Matrix of Fields](#)

Variable: `hdr_exeter` Branching logic: `[record-dag-name]='26_exeter'` [How to embed a field](#)




[Add Field](#) [Add Matrix of Fields](#)

Variable: `hdr_southern` Branching logic: `[record-dag-name]='40_southern'` [How to embed a field](#)



[Add Field](#) [Add Matrix of Fields](#)

Variable: `hdr_worcestershire` Branching logic: `[record-dag-name]='17_worcestershire'` [How to embed a field](#)



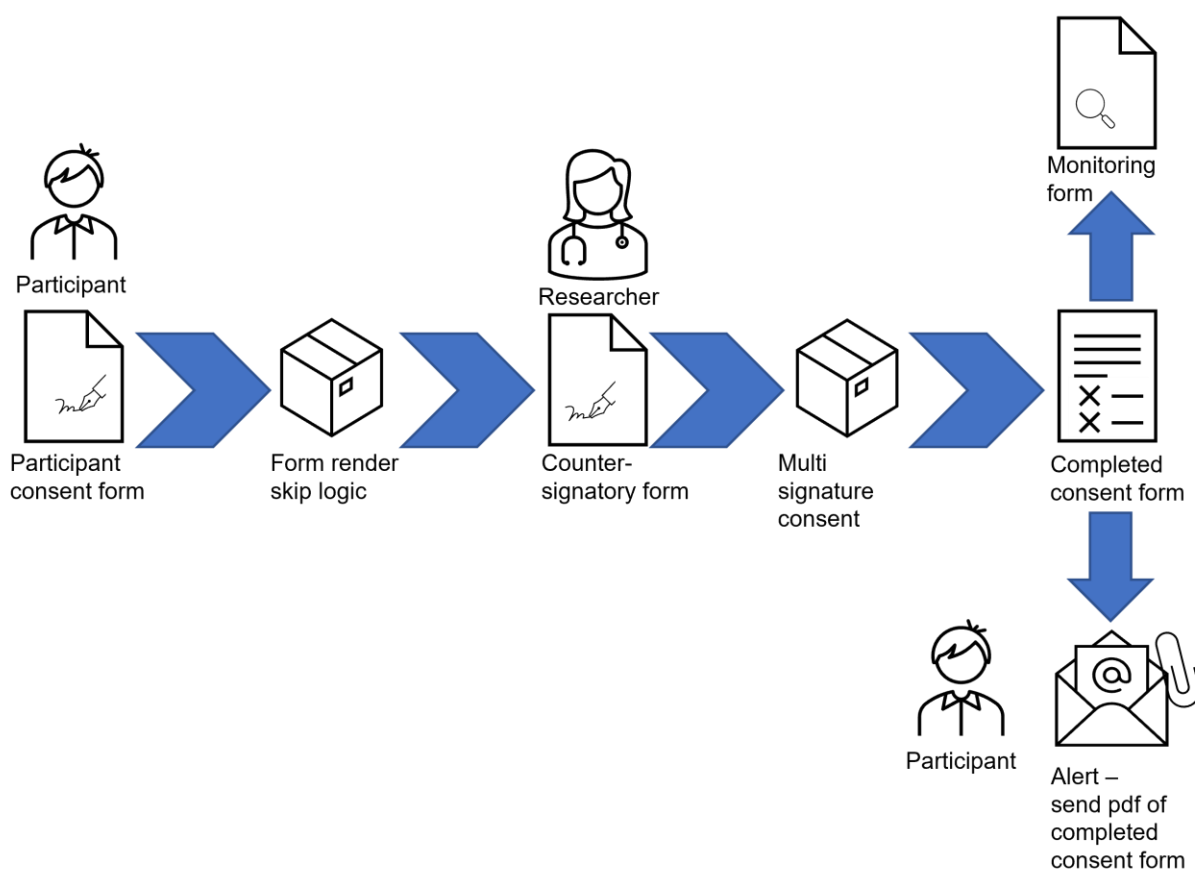
This is fairly simple to implement, although it's worth noting that the admin overhead grows with the number of sites, so make sure you resource the study accordingly.

Countersigning

As mentioned above, we often have a requirement for a researcher to be able to countersign a consent form to document that they have witnessed it.

We suggest using a separate form for countersigning, as this creates a clearer workflow and enables you to set permissions on the form appropriately. It also removes the risk of the researcher accidentally overwriting the participant's consent form, which can happen if the same form is used for participant consent and researcher countersigning.

You can then use the **Form Render Skip Logic** EM to hide the countersignature form until the participant has completed their consent form, and the **Multi signature consent** EM to merge the two forms into a single PDF.



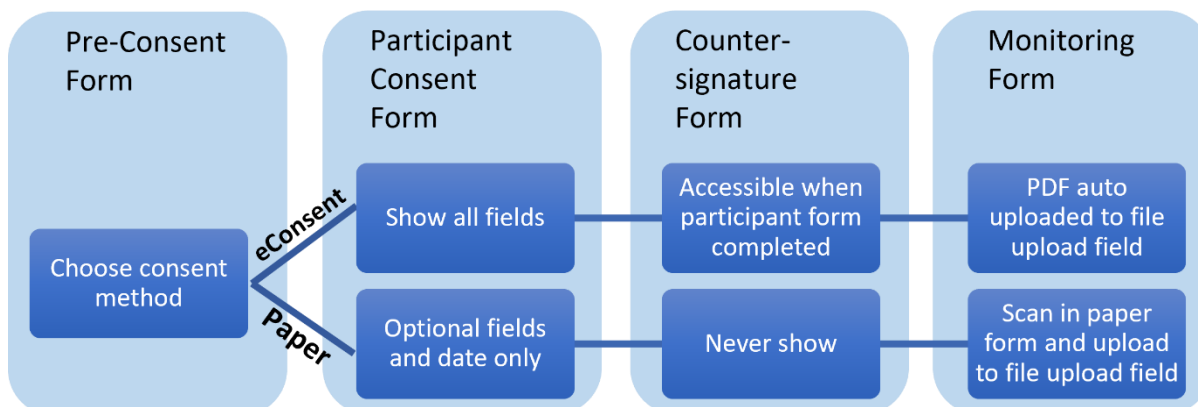
Hybrid Paper and eConsent

To implement hybrid paper and eConsent, we suggest the following:

Create four forms:

- **Pre-consent form**, recording whether consent will be eConsent or paper, and drop down list with the version of PIS and ICF being used
- **Participant consent** form – branching logic to show all questions if eConsent, and only optional consent questions and consent date if paper consent

- **Countersigning** form – only shows if eConsent selected AND participant signature and name are in consent form
- Consent form **monitoring** page – has two upload fields, one for eConsent and another for paper, which show depending upon which option selected in pre-meeting form, and fields to record the date reviewed by the monitor.



You may wish to keep the eConsent form just as an eConsent form, and add a separate form to store the consent date and optional items for participants who have completed on paper. This has the advantage that you can make the eConsent form read-only for researchers, which reduces the risk of accidental overwriting. The disadvantage is that the date and optional items will be stored in separate fields for the electronic and paper consent participants.

8. General Considerations and known issues

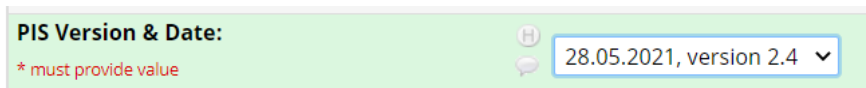
Here are some general considerations and common issues you might run into/want to try to mitigate

New PIS versions/updates during study/maintenance

It is likely that you will need to update the PIS and/or ICF during the study, releasing a new version for sites to use.

This can be implemented in the eConsent system as follows:

1. Add a drop-down list of PIS versions to the pre-consent form in REDCap. The researcher should select the version given to the participant prior to consent.



2. You can then use piping in REDCap to display this version in the text of the consent form. This will be displayed to the participant during consent, and will be saved in the database as part of their record, and included in the PDF copy.

1. I confirm that I have read and understand the participant information sheet dated 28.05.2021, version 2.4 for the above study and have had the opportunity to ask questions.

* must provide value



- As versions of the PIS are retired, they can be hidden on the dropdown list using the @HIDECHOICE action tag. This means that existing values will remain in the database, but older PIS versions will not be available for new records

Choices (one choice per line)

2_3, 23-03-2021, version 2.3
2_4, 28.05.2021, version 2.4
2_5, 28.07-2021, version 2.5

Action Tags / Field Annotation

@HIDECHOICE='2_3'

Re-sending consent form links

A common issue with remote eConsent is the emails containing the link to the consent form not arriving with the participant. This is usually either because the wrong email address was entered, or because the email got caught in the participant's spam filter.

If you are using ASIs to send your consent form links, there is no particularly easy way to re-send them. Re-sending an email involved several steps

If you use ASIs, there is an easier way:

- Set the ASI to send immediately when the contact details form is saved
- Set it to re-send every time the contact details form is saved with modified data

This way, the user corrects the email address and saves the contact details form to re-send the email.

It's advisable to add some logic to only send the email if the consent form has not yet been completed, as you want to avoid sending repeated emails to the participant any time their contact details change.

Preventing participants from consenting twice

The question came up during our webinar series of how to prevent participants from consenting more than once.

This depends on how your eConsent system is set up.

Broadly speaking there are two scenarios to consider:

- Participants added to the database by a researcher
- Open online recruitment

Participants recruited by researcher

The first thing would be to decide how you can identify participants. You would need to select one or more fields that you were confident would be unique to the participant. Email address and or

mobile phone number would be good candidates. You could check on a combination of first and second name, but this is less reliable.

Once you have selected the fields that you want to use, you can install the **Check for Duplicates Across Multiple Projects** External Module. This will flag up a warning if the researcher enters duplicate values for these fields that are already in the database.

Open online recruitment

Preventing duplicate consents is more challenging in a study using open online recruitment. The bottom line is that it may not be possible to prevent duplicate consents entirely.

Custom code can be written to detect duplicate contact details during sign-up, and flag this in a hidden field. You can then divert the participant to a 'thanks but you have already consented' page using the Autocontinue logic external module.

It is worth bearing in mind that you may not necessarily want to prevent participants from consenting twice in this scenario. For example, if the process is that the participant consents, completes baseline questionnaires and is then randomised, it is possible that the participant might be interrupted or lose internet connection during their baseline questionnaires, and need to go back and start again. It may be better to focus on preventing them from being **randomised** twice, rather than consenting twice.

9. Where to get help

One of the major benefits of using REDCap as an eConsent platform is that a large amount of help and support is available.

REDCap community forums

REDCap has a large and highly active and supportive community with over 2 million users worldwide at over 5815 institutions in 145 countries (<https://projectredcap.org/> accessed 15/03/2022).

Joining the REDCap consortium gives you access to an online forum where you can

- Ask for help setting up your REDCap install
- Ask how to achieve specific functions within your redcap projects
- Suggest and vote on new features for the developers to include in the software

Members of the forum are very quick to respond to questions, often answering them within a day or two.



Note: REDCap Forum access is limited to **5 users per instance**, and is intended only for the admins who manage the REDCap instance at your institution. Normal REDCap users will not be able to access the forum. We'd suggest setting up a REDCap user group within your institution to help share knowledge.

The community also creates and shares 'External modules' which you can download and plug into your REDCap install to add extra functionality.

UKCRC REDCap user group and Trialaborate

The UKCRC runs a REDCap User group for IS teams from UK CTUs. They meet regularly, and post shared resources on the Trialaborate forum.

Online

Many of the institutions that user REDCap have made their help documentation available online. A quick web search on 'REDCap eConsent' will reveal dozens of pages of results.