Virtual and e-consent in Research at NuTH

NJRO-GEN-SOP-028

Contents

1. Background/Introduction

Electronic methods for seeking, confirming and documenting informed consent (otherwise termed 'e-consent') are becoming increasingly popular in research, either to supplement the traditional paper based approach to consent, or where appropriate, replace it. Remote/virtual methods for seeking, confirming and documenting informed consent are also becoming more common. The Health Research Authority (HRA) and Medicines and Healthcare products Regulatory Agency (MHRA) have subsequently published a joint statement on seeking consent by electronic methods (September, 2018). Whilst the statement focuses primarily on clinical trials, the basic principles can be applied to all research conducted within the UK when consent is sought via electronic means.

Researchers however should be mindful that the use of e-consent may unintentionally discriminate against those who are not comfortable or who cannot use such technology (such as those who have a lack of familiarity with electronic systems, poor eyesight or impaired motor skills), therefore alternative methods for the provision of information and/or documentation of consent should be available for those who are unwilling to use electronic methods (HRA & MHRA Joint statement, 2018). There are however potential advantages of using e-consent systems, such as improving the informed consent experience by offering an interactive and engaging approach; rapid notification of amendments to participants that may impact their willingness to participate; and the promotion of timely e-consent data entry.

2. Purpose

The purpose of this SOP is to describe the methods and principles for seeking, confirming and documenting informed consent by electronic means (e-consent) at NuTH. Many principles within this SOP may also apply to remote/virtual consent.

Throughout this SOP, e-consent refers to the use of any electronic media such as text, graphics, audio, video and websites to convey information related to the study and to seek and/or document consent via electronic devices such as smartphones, tablets or computers.

3. Scope of Document

This SOP is applicable to researchers and support staff seeking, confirming and documenting e-consent/remote consent for studies sponsored and hosted at NuTH.

This SOP is also applicable to all NJRO staff that provide guidance and support on hosted research at NuTH.

This SOP is also applicable to all NJRO and trial management staff who work on NuTH sponsored research, where the CI wishes to utilise appropriate e-consent or virtual/remote consent methods (with agreement from sponsor) within their research.

4. Definitions

CTIMP: Clinical Trial of an Investigational Medicinal Product
e-consent: electronic consent
e-signature: electronic signature
HRA: Health Research Authority
ICF: Informed Consent Form
MHRA: Medicines and Healthcare products Regulatory Agency
NuTH: Newcastle upon Tyne Hospitals
PIS: Patient Information Sheet
RCT: Regulatory Compliance Team

5. Roles & Responsibilities

It is the responsibility of all research staff delegated the task of receiving consent to ensure they read and follow this SOP when utilising e-consent or virtual/remote consent methods.

It is the responsibility of NJRO sponsor representatives to ensure any e-consent/remote consent methods proposed in NuTH sponsored studies comply with this SOP, and that any methods are risk assessed (with risk mitigations proposed) where appropriate.

The RCT within the NJRO are responsible for overseeing the vendor assessment process for any third party providing e-consent services in NuTH sponsored high risk trials.

6. Procedures

6.1. Electronic Signatures

The UK eIDAS Regulations (SI 2016/969) defines an electronic signature as '*data in electronic form which is attached to or logically associated with other electronic data and which is used by the signatory to sign*'.

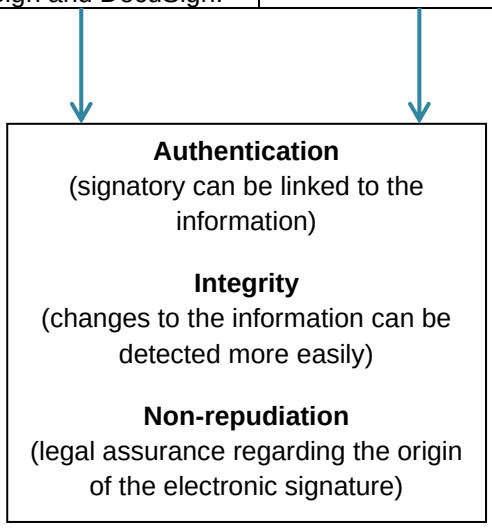
The MHRA GxP Data Integrity Guidelines and Definitions (Revision 1, March 2018) define an electronic signature as: '*A signature in digital form (bio-metric or non-biometric) that represents the signatory. This should be equivalent in legal terms to the handwritten signature of the signatory.'*

Electronic signatures may include tick box plus declarations; typewritten; scanned; electronic representation of a handwritten signature; unique representation of characters; digital representation of characteristics (e.g. fingerprint); and a signature

created by cryptographic means. However, the type of electronic signature required for e-consenting in research varies depending upon the nature, complexity and risk of the trial.

Electronic signatures can be defined in to 3 groups:

Simple	Advanced	Qualified
E.g. stylus or finger drawn signature; typed name; tick box and declaration; unique representation of characters; fingerprint scan.	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. Examples include AdobeSign and DocuSign.	An advanced electronic signature, uniquely linked to the signatory, that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.



Some electronic signatures are more reliable and provide greater assurance than others. For instance qualified electronic signatures are automatically granted the legal effect of a handwritten signature with mutual recognition throughout EU (HRA & MHRA Joint statement, 2018).

The method of authentication of electronic signatures used in a study should be proportionate to the nature/complexity of the research; the risks, burdens and potential benefits; and the ethical issues at stake.

Key considerations in identifying an appropriate risk based and proportionate e-consent process will include: Does your recruitment and consent procedures mean that you can:

- Trust that the person who signed is who they say they are (i.e. ensuring that the signature is attributable to the individual)
- Trust that the consent form they signed hasn't been altered (i.e. ensuring that the act of 'signing' is recorded within the system so that it cannot be altered or manipulated without invalidating the signature or status of the entry)
- Trust when the signature was applied (i.e. ensuring the signature is date stamped)
- Trust the security of the electronic signature (i.e. ensuring that it can only be applied by the 'owner' of that signature).
- Adequately demonstrate that trust is justified if required e.g. during an inspection/audit (i.e. ensuring the record of the signature can be associated with the entry made and how this can be verified with a full audit trail).

When considering the implementation of electronic signatures, it is important to consider if any patient identifiable data would be stored or accessible outside the site and the security of this data.

Any methods of e-consent and electronic signatures must be approved by the sponsor and the REC/HRA. Regardless of whether paper-based or multimedia formats are used, the process of obtaining voluntary and informed consent must be upheld in accordance with the principles of GCP and all regulatory requirements.

6.2. Seeking e-consent/remote consent in CTIMPs

6.2.1. Provision of Information in CTIMPs

The methods used to inform and document the consent of participants in CTIMPs must comply with The Medicines for Human Use (Clinical Trials) Regulations 2004 (as amended).

Participants must be provided with information on the nature, significance, implications and risks of the trial and the right to withdraw from the trial at any time. A contact for further information (such as the local principal investigator) must also be supplied.

Participants must be provided with information by interview with the investigator or a member of the investigating team. This enables potential participants to understand the nature, significance, implications and risks of the trial so they are able to make an informed decision about whether or not to partake. Simply providing potential

participants with this information (by paper or electronic means) would not be considered an interview; this requires an interactive process that enables participants to ask questions and receive answers from the investigating team.

The interview should be conducted in person where possible, or where justified (and approved by a REC), by electronic methods that allow two-way communication in real time. Whichever method is used, it is essential that confidentiality is maintained, the communication method is secure and the method has been approved by the sponsor, REC and NJRO.

Investigators should (where possible) align with local practice at sites for e-consultations when setting up an interview for e-consent/remote consent. For instance 'Attend Anywhere' is an online service which is utilised in routine practice for video call appointments at NuTH.

Whichever method is used, it should facilitate thorough and interactive communication that enables the potential participant to understand what participation would involve. It should also allow for the confirmation of the participant's identity, particularly where the interview and documentation of consent are carried out by electronic means at a distance.

In trials where face-to-face verification is not possible, for example where the trial is to be conducted entirely remotely, the participant's identity may be verified visually via a video link (and asking the patient to confirm their name and date of birth) or other means. It may also be possible to utilise general practices or other NHS sites local to the participant in order to verify their identity. Please note: the conduct of a CTIMP remotely would need to be approved by both the MHRA and a recognised REC.

Where the e-consent process takes place at a research site, verification of the participant's identity should be no more burdensome than it would be for a traditional hard copy consent process.

Although it is not a legal requirement to provide study information in writing (whether this refers to a hard copy or digital PIS), potential participants (and/or their legal representative where appropriate) should be provided with access to written information about the study for the purpose of seeking informed consent, either as a physical hard copy or digital download. Participants can then use this in conjunction with the interview to help them reach an informed decision.

Participants (and legal guardians where appropriate) should also be provided with a copy of (or have access to) their signed and dated consent form (either electronically or on paper).

Where a hardcopy of the information is provided via an e-consent system, this must contain sufficient information regarding the nature, significance, implications and risks of the trial and explain the participant's right to withdraw at any time. However the hardcopy PIS does not need to reproduce multimedia content contained in the e-consent information.

6.2.2 Recording consent in CTIMPs

For CTIMPs, the participant's (or legal representative where applicable) consent must be recorded in writing, dated and signed, or otherwise marked by the participant. 'Writing' is defined in UK law as 'typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form'. It does not necessarily have to be on paper.

Where the participant has capacity but is unable to indicate their consent by signing (either by wet ink or electronic signature) then their consent may be given orally in the presence of at least one witness and recorded in writing. This method must be approved by a REC.

6.2.3 Electronic signatures in CTIMPs

The type of electronic signature that should be used will depend upon the specific context and risk of the trial.

For most CTIMPs (and other research involving more than minimal risk/burden/intrusion), simple e-signatures that involve the participant tracing their handwritten signature using a finger or a stylus or biometric e-signatures should normally be used as they allow for direct comparison with e-signatures and/or wet ink signatures previously used by the participant for the purpose of audit or where the consent is contested.

For type 'A' CTIMPs (where the risk is no higher than that of standard medical care) any simple e-signature may be used. This may involve the participant tracing their handwritten signature using a finger or stylus or biometric e-signatures. Typewritten or scanned signatures may also be used with sponsor and HRA/REC approval. Regardless of the use of a simple e-signature, verification of the participant's identity must be confirmed.

For type B (where the risk is somewhat higher than that of standard medical care) and type C (where the risk is markedly higher than that of standard medical care) trials, simple e-signatures (e.g. finger drawn stylus or biometric e-signature) may be used however typewritten or scanned images must not be used. Verification of the participant's identity must be confirmed. Where the participant is not known to the

research team, there should be an auditable trail to demonstrate trust of the identity of the signatory.

A specific situation or type of trial may require the use of 'advanced' or 'qualified' electronic signatures in order to provide greater assurance that the documentary evidence does indeed represent the consent of the specific participant it purports to (e.g. where the trial is to be conducted entirely remotely and face to face verification is not possible).

Where consent is given remotely the investigator should ensure the e-consent process allows for discussion and ample opportunity to ask questions. This may utilise phone calls or secure video consultations (e.g. via 'Attend Anywhere'). If the participant is required at some point to visit the site for study purposes, then verification can be done in person provided this is done prior to receiving any intervention (this should be documented in the patient records). If clinical trial activities are solely conducted remotely, it may not be possible to verify who the participant is in person, therefore an advanced or qualified e-signature should be used.

The HRA/MHRA joint statement provides examples of e-consent scenarios for: 1) a Type B or C CTIMP where the consent process takes place in person at site and 2) CTIMP where the patient is remote at the time of consent.

6.2.4 Some additional conditions for using electronic methods to seek and document informed consent in CTIMPs (please note some points below apply to all research – this has been clearly indicated)

- The signature must be dated either manually by the participant or automatically by the e-consent system (applies to all research)
- Non-editable copies of the PIS/ICF should always be provided to participants. It must be possible to verify which version of the PIS and ICF the electronic signature applies to (applies to all research)
- Methods must be in place to ensure that the person signing the electronic consent form is the person who will be participating in the research study (applies to all research)
- The source consent documentation (including audit trails and metadata) must be stored in the ISF and must be available for inspection during and after the end of the trial according to the legally required retention period
- Access to the e-consent system must be readily available to auditors, inspectors and monitors both during and after the end of the trial (applies to all research)
- The site team must be able to retain control of the informed consent process and documentation so that personal identifiable data are not inappropriately disclosed beyond the site to sponsors or third parties (applies to all research)

- Where a sponsor has commissioned a third party to provide an e-consent system, the necessary information governance arrangements must be in place to ensure participant confidentiality is protected with appropriate access and retention controls to the system. Where the sponsor is responsible for auditing, ensuring compliance, and maintaining access controls to the e-consent system they may provide the appropriate certifications to the site as needed (applies to all research)
- Personal identifiable data should not be disclosed beyond the site unless explicit agreement has been sought from the sponsor, local site and the patient has consented to this. GDPR and local policies must be followed (applies to all research)
- A copy of the informed consent documentation (PIS & ICF) must be provided to the participant and retained in the ISF (applies to all research)
- MHRA inspectors must be able to access the e-consent system in a readily available way during triggered, short notice or unannounced inspections.
- Where advanced or qualified electronic signatures have been used, an inextricable link must be maintained between the metadata and the document, thus demonstrating the electronic signatures authenticity for as long as applicable legislation requires, dependent on the type of trial.

6.3. Seeking e-consent/remote consent in other research

For non-CTIMPs, although it is not a legal requirement to provide written information or document consent in writing, it is considered best practice and so investigators must document consent unless not doing so can be justified (and approved by the sponsor, NJRO and a REC).

Participants with capacity who are unable to physically sign a paper or electronic document may provide consent orally or by any other means of communication. Again this must be approved by the sponsor and a REC.

6.3.1 Electronic signatures in non-CTIMPs

For the majority of non-CTIMP research involving only negligible or minimal risk (e.g. face to face surveys / non-sensitive qualitative research), any simple electronic signature is normally adequate where it is approved to seek consent (including typewritten or scanned e-signatures).

Where the research involves more than minimal risk/burden/intrusion simple e-signatures that involve the participant tracing their handwritten signature using a finger or stylus or biometric eSignature should be considered as they allow for direct

comparison with e-signatures and/or wet ink signatures previously used by the participant.

For postal/online surveys or self-administered questionnaires where identifiable personal data are collected, and consent used as the legal basis for the purposes of GDPR compliance, then the participant must be able to actively signify their consent. This can be achieved by providing an explicit consent statement and a tick box within the survey/questionnaire that the participant can complete if they are in agreement. A handwritten/biometric eSignature is not necessarily required.

6.4 Use of e-consent/remote consent in NuTH sponsored studies

If a CI wishes to incorporate e-consent/remote consent in to their study design, this must be highlighted to the NJRO sponsor team before any funding application is submitted. It should be made clear when completing the Project Initiation Form (PIF) which is then reviewed by the NJRO sponsor team. The sponsor team can then assess the feasibility of using e-consent/remote consent within the proposed study which will also feed in to whether provisional sponsorship can be confirmed. Some aspects to consider when reviewing an e-consent method from a sponsor perspective are included within Appendix 1, although please note this is not an exhaustive list.

The time needed to develop and set up e-consent/remote consent processes should be factored in to the study setup timeline. For instance, the CI should consider additional time for any necessary vendor assessments, contracting, e-consent system development, validation and user acceptance testing, appropriate site feasibility assessments, e-consent training etc. The sponsor team can advise on this during application meetings or via email as appropriate.

Electronic methods for seeking informed consent must be documented in the study protocol and appraised at the study risk assessment. Appropriate risk mitigations will be implemented by the sponsor team, which may include the development of a QA strategy (e.g. application of a computer system validation review for an e-signature / audit of the e-consent process) and/or monitoring strategy (e.g. targeted monitoring of the e-consent/remote consent process).

If CI's wish to utilise any third party vendors as part of e-consent provision, approval must be sought from the sponsor team. The sponsor team will conduct a vendor assessment where appropriate. Some aspects that will be considered within the sponsor vendor assessment include:

- Vendor policies and procedures for storing and archiving approved documents
- Data security, access & storage (only the site should have access to signed consent forms)

- Ability to access paper based versions of e-consents
- Audit trail – capture revisions, person making changes, reason for changes and date the changes were made.

It is also important that any e-consent/remote consent methods contain appropriate version control so it is clear what version of the consent form has been signed and when, and also what PIS version the patient has received.

All versions of the e-consent form should be available throughout the study and following archiving for monitoring, audit and inspection purposes. Similarly, if patients are required to re-consent throughout the trial, all versions of e-consent forms signed should be available and accessible.

It is also vital to incorporate contingency planning within the study risk assessment / monitoring plan (as appropriate) to ensure that if technical disruptions or failures arise in relation to the e-consent system, there is a contingency plan for the consent process.

Appropriate e-consent/remote consent training for sites is also vital during the site set up process and should be incorporated in to Site Initiation Visit (SIV) information. All relevant staff must be trained on the e-consent/remote consent process before sponsor green light can be given.

The acceptability of e-consent/remote consent methods at site level must be explored within the site feasibility assessments. The use of e-consent/remote consent is still quite novel throughout the NHS therefore different sites may have different requirements and capabilities.

It may be useful to develop an e-consent/remote consent manual for sites to use, which may detail the process for user training/certification; process for consent printing; process for archival; contact information for assistance; and back up process in case of system failure.

7. References

EU regulation No 910/2014 is supplemented by the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (SI 2016/696) (the UK eIDAS Regulations) as amended.

HRA & MHRA: Joint statement on seeking consent by electronic methods. V1.2. September 2018. Available at: < https://www.hra.nhs.uk/about-us/news-updates/hra-and-mhra-publish-joint-statement-seeking-and-documenting-consent-using-electronic-methods-econsent/>

MHRA GXP Data Integrity Guidance and Definitions. Revision 1, March 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

TransCelerate Biopharma eConsent Implementation Guidance. V1.0 (2017) http://www.transceleratebiopharmainc.com/initiatives/econsent/

U.S. Food and Drug Administration. Use of Electronic Informed Consent in Clinical Investigations, Questions and Answers. Guidance for Institutional Review Boards, Investigators, and Sponsors (December 2016) https://www.fda.gov/downloads/drugs/guidances/ucm436811.pdf

8. Appendices

Appendix 1 - Some sponsor considerations when reviewing an e-consent/remote consent system (please note this is not an exhaustive list):

Operational Considerations
Both electronic and paper based process available to use? Ability to document process used in EDC system? Can the EDC system highlight any non-compliances with the e-consent process? Access to ICF browser independent if patients are expected to use their own devices? Provision of devices clear and appropriate (if appropriate)? Access to ICF browser if activity is taking place in patient homes or on site? Is there a contingency plan in case the e-consent system experiences technical failures? Does the e-consent process involve an interview with participants where required and does this align with local e-consultation methods at sites? Does e-consent/remote consent align with the visit schedule? (e.g. consider if the participant needs to attend hospital for baseline visits and thus whether remote consent is an appropriate option, or whether this can be done on site)
Roles and Responsibilities
How is version control managed with regards to the e-consent documentation? How are different languages managed (where appropriate)? Who is hosting the eICF software application and is a vendor assessment required? Are appropriate information governance arrangements in place to protect participant confidentiality? How is website access controlled? How are questions created and answered? What happens if the website is down temporarily? Who is managing the user accounts and are these issued only after e-consent training?
Subject Authentication
Can the signature be attributed to the person participating in the trial and can this be demonstrated via audit trail for inspection purposes? Is there a verification step to ensure this? Subject cannot repudiate/delete the signature once invoked? Any person cannot alter the consent form once fully signed? Signatures time/date stamped, either manually by the participant or automatically by the e-consent system? Can the electronic signature only be applied by the owner of that signature? Is it possible to verify which version of the PIS and ICF the electronic signature applies to? Is there ongoing opportunity to document continued consent?
Accessibility
Appropriate access and retention controls in the e-consent system? Is the eICF printable as a non-editable PDF?

Can the patient access a non-editable copy of the PIS (containing information on the nature, significance, implications and risks of the trial, and right to withdraw from the trial at any time) and ICF? Do patients have a contact for further information about the trial? Can you ensure the patients had enough time to consider the trial? Can this be accessed for monitoring, audit and inspection purposes at short notice? Can source consent documentation (including audit trails and metadata) be stored in the ISF and be available for audit/inspection purposes? Is access to the e-consent system readily available to auditors, monitors and inspectors both during and after the trial? Can the site team maintain control of the informed consent process/documentation so that personal identifiable data are not inappropriately disclosed beyond the site to sponsors and third parties?
Other Is it feasible/appropriate to use e-consent/remote consent in the study population? (i.e. e-consent methods should not discriminate against those who are not comfortable or who cannot use such technology) Consider whether sufficient time has been factored in to the setup of the study to develop the e-consent system and conduct all necessary sponsor assessments? Has the feasibility of e-consent been assessed with sites? Is contracting/vendor assessments required with third party e-consent providers? Is an assessment needed from information governance? Validation and user acceptance testing considered? Has a sufficient e-consent/remote consent training package been developed? Is the e-consent/remote consent process appropriately documented throughout the study documentation (e.g. protocol, application, PIS, risk assessment, monitoring plan etc.)? Is an e-consent study manual required? Does the e-consent/remote consent process comply with the principles of GCP? Has the e-consent system been appropriately costed (where appropriate)? (consider any financial impact on the funding application/grant)