

# Electronic Consent Guidelines

## **Obtaining and Documenting Consent Electronically**

Article 3.12 of the TCPS2 states that evidence of consent shall be contained either in a signed consent form or in documentation by the researcher of another appropriate means of consent.

In studies regulated by Health Canada (usually clinical trials), consent must be visible – either written or electronic. Health Canada can waive this requirement but this is considered on an individual case basis, negotiated between the Investigator/Sponsor and Health Canada. In other studies, alternate means are acceptable. For example, studies seeking consent to use health information for research purposes may seek consent that is either written or electronic. This guidance describes electronic methods of informed consent documentation.

Electronic documentation of consent may be used when researchers conduct the consent process with participants in person, as well as when potential participants are not physically present with the researcher during the consent process. In either situation, the consent process itself should be designed to ensure that participants are adequately informed about the research, can easily ask and get answers to questions, and recognize that participation is voluntary. The REB must consider how the electronic signature is being created, whether the signature can be shown to be legitimate, and how the research team plans to provide a version of the consent form to the potential participant for their review and retention.

## **Types of Electronic Signatures**

When providing consent online, there are a number of ways in which an e-signature might be documented. Some examples include:

- Signing with a stylus in an electronic document
- Attaching a scanned handwritten signature or using an e-signature service such as REDCap. The following e-signature services have undergone privacy and security review by the University and are considered acceptable; REDCap, SignNow and DocuSign. (Other platforms may be

acceptable but the researcher must demonstrate that they meet all privacy and security requirements of the University of Alberta.)

- Typing one's name with an accompanying check box and statement noting an intent to affix a legal signature (e.g., "By checking this box and typing my name below, I am electronically signing this consent form")
- All of the above constitute "signatures."

### **Capturing Signatures Electronically**

The REB permits in-person consent to be executed and stored using electronic devices (e.g., tablet or iPad). In the case where this type of electronic consent is used, the person obtaining consent must witness the study participant as s/he provides her or his electronic signature and must then provide her or his own electronic signature. The provision of consent will thus be witnessed and both parties' signatures will be on the consent document.

The electronic version of the consent document should be stored, accessed and transmitted according to the University of Alberta Guidelines. For example, when using a tablet, the consent form should not be stored on the actual device but downloaded to secure UofA/AHS servers. Access to the consent form should be at least as closely guarded as access to paper consent forms. Both the electronic version of the consent and paper versions subsequently generated by the researchers are to be considered originals.

### **Signatures Transmitted Electronically**

#### **Faxing Copies of Signed Consent Forms**

It is permissible for participants to fax a signed copy of the consent form to the research team. If there are questions and/or check boxes embedded throughout the document for the participant to complete, the research team should check to ensure that these pages are included. Some standards (e.g., ICH GCP) guidelines require that the study team receive a complete copy of the signed consent form. In cases where participants are faxing a consent form to the research team, the participant need not provide the investigator with the original signed consent document. Privacy concerns to be addressed include how the fax machine is monitored/who has access and the nature of the information contained in the consent, recognizing this could be both sensitive and identifying.

#### **Emailing Copies of Signed Consent Forms**

Researchers often want to send a consent document via email. In the case of health-related research, it is the opinion of the REB and the Institutional Privacy Advisor that the information contained in a consent form combined with the email address of the recipient (often first and last name) can inadvertently link a diagnosis with an individual. As such, the REB believes this should be considered indirectly identifying health information. It may be permissible, however, to send a consent form via email if it is encrypted (ie. Encrypted .pdf document). The encryption code should be a strong code and it must be sent to the participant separately from the email (ie. Telephone conversation). In the case where the participant is to sign the document and return it to the study team, the encryption of the document needs to persist after the document is opened – (i.e. automatically revert to its encrypted form once closed). Consent forms sent via a secure AHS email account meet these encryption requirements. So long as the recipient returns the consent form within the same email thread, AHS has advised that the encryption remains. The email which contains the encrypted consent document should also contain explicit language that the research participant should NOT communicate any questions related to the consent document back to the researchers via email. A script as to the contents of this email should be provided to the REB as part of the application.

### **Sending a link to a secure database that holds a consent form**

Researchers may be using a system (like REDCap) which can hold documentation like a consent form, study questionnaires and/or participant documents. The REB would approve of the use of email to inform participants that such documents are available to them, through a link into the secure website. This will be evaluated on a case by case basis and be dependent on the secure system being used.

### **Confirming Identities in Online Research**

A study's data validity or reliability could be questioned if participants' identities are not verified/verifiable. Examples include when there are critical eligibility criteria, or when there is a likelihood of repeat or fraudulent participation, whether for mischief or to collect multiple payments. When designing a research study, investigators should take into consideration the importance of establishing participant identity to their study.

Studies that pose more than minimal risk, or that involve the transmission of health information, should consider implementing a process by which the study team confirms identities using authentication that relies upon multiple factors, for example a password that is delivered to participants by telephone or by postal service.

### **Example Text for Ethics Applications That Use REDCap**

The Health Research Ethics Board and REDCap have collaborated to ensure that a consent process within REDCap would meet the regulations set out in the Health Information Act. The following text is appropriate to include in your ethics application. It should describe how you plan on identifying the participant AND how you know that it is the participant that is actually completing the form.

*Participants are contacted by telephone using the contact telephone number contained in their electronic medical record. During the call, the participant is identified by asking them to provide their date of birth and provincial healthcare number. These are verified by comparing them with the data in the participant's electronic medical record. Once the participant has been identified they are registered in REDCap and REDCap emails them a link to the eConsent form. The link in this email contains a token, which is unique to that study participant. The participant clicks the link and completes the eConsent form while still on the phone with the study coordinator.*

If you are using a password then this text is more appropriate...

*Participants are contacted by telephone using the contact telephone number contained in their electronic medical record. During the call, the participant is identified by asking them to provide their date of birth and provincial healthcare number. These are verified by comparing them with the data in the participant's electronic medical record. Once the participant has been identified they are registered in REDCap. REDCap generates a unique password and emails the participant a link to the eConsent form. The link in this email contains a token, which is unique to that study participant. The participant clicks the link, logs into REDCap using the password provided by the coordinator, and completes the eConsent form while still on the phone with the study coordinator.*

These processes may also be applicable to other platforms but would be evaluated on an individual case basis.

## **Online Consent**

### **Implied**

For minimal risk research such as web-based surveys or questionnaires, the consent form may be presented online, and require participants to perform some action, such as clicking “I agree,” before proceeding with any research activities (e.g., answering survey questions on a website). This is an acceptable approach for minimal-risk research conducted online and is considered an implied consent. Where participation in an online survey is anonymous, it is acceptable to include a statement in the information letter indicating that submission of the survey implies one’s consent to participate.

## **Consent statement**

For studies where the informed consent document is provided online, consent may be documented by the participant typing their name with an accompanying check box and statement noting an intent to affix a legal signature (e.g., “By checking this box and typing my name below, I am electronically signing this consent form).

The research team should consider how they will be able to evaluate a participant’s understanding of the procedures and risks related to their participation, particularly where the research involves more than minimal risk. Contact information for a member of the study team must be provided so that potential participants can have questions or concerns addressed. A brief quiz to assess the potential participant’s understanding of the study, including their role, the risks and benefits and confidentiality provisions might also be useful for more complex studies.

## **Providing Participants Copies of Consent**

In all cases where consent is obtained and documented electronically, participants must be provided with a version of the consent form that they can retain for their records, whether it is a hard copy or an electronic version.

## **Additional Resources and Web Links**

1. TCPS (see Chapter 3): [https://ethics.gc.ca/eng/tcps2-eptc2\\_2018\\_chapter3-chapitre3.html](https://ethics.gc.ca/eng/tcps2-eptc2_2018_chapter3-chapitre3.html)
2. Health Information Act of Alberta: <https://www.alberta.ca/health-information-act.aspx>
3. Health Canada (Guidance for Clinical Trial Applications): <https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/applications-submissions/guidance-documents/clinical-trials/clinical-trial-sponsors-applications.html>
4. ICH GCP (see Section 4.8): [https://database.ich.org/sites/default/files/E6\\_R2\\_Addendum.pdf](https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf)
5. FDA (guidance on use of electronic consent):  
<https://www.fda.gov/downloads/drugs/guidances/ucm436811.pdf>
6. Use of Email to Communicate with Study Participants Guidance:  
<https://www.ualberta.ca/research/media-library/reo/human-ethics-files/forms-files/2019-02-01-use-of-email-guidance.pdf>
7. UofA REDCap Supports – Regarding Electronic Consent: <https://help.redcap.ualberta.ca/policy-procedure/electronic-consents>
8. The development of this document was informed by that of the University of Calgary:  
<https://www.ucalgary.ca/research/files/research/chreb-guidance-electronic-consent-02feb2018.pdf>