COLUMBIA UNIVERSITY
INSTITUTIONAL REVIEW BOARD

GUIDANCE ON ELECTRONIC INFORMED CONSENT FOR RESEARCH

I. BACKGROUND

This document provides guidance to researchers at Columbia University (**Columbia)** on the use of electronic systems and processes to obtain and document informed consent for research. It also describes several systems available for researchers to facilitate electronic informed consent (**e-Consent)**, and their pros and cons.

Federal regulations for the protection of human subjects in research support the use of e-Consent and e-Signatures (as defined in Section III (A) below). The Food and Drug Administration (**FDA**) requirements for electronic records/electronic signatures, informed consent, and IRBs are set forth in 21 CFR Parts 11, 50, and 56, respectively. The U.S. Department of Health and Human Services (**DHHS**) requirements for information presented to a research subject, processes used for obtaining informed consent, and documentation of electronic informed consent are set forth in 45 CFR Part 46 and other applicable regulations.

II. EFFECTIVE DATE: June 11, 2021.

This Guidance replaces the Columbia University Institutional Review Board Guidance on Electronic Informed Consent, dated May 1, 2017.

III. E-CONSENT

A. Definitions

Electronic Consent (e-Consent): the use of electronic systems and processes, whether in person or remotely, that employ electronic media (e.g., text, graphics, audio, video, podcasts, websites) to convey information relating to a research study and/or to document informed consent of subjects who wish to participate in such study.

There are two types of e-Consent: In Person and Remote.

In Person e-Consent: the person obtaining consent (**POC**) and the potential research subject are physically in the same location, the consent discussion occurs in person, the consent document may be presented electronically (e.g., via an iPad or tablet) and/or may be signed electronically if documentation of consent is required.

Remote Consent: the potential participant reviews the consent document in the physical absence of the POC, the consent process may involve web-based software, email, postal service mail, or a mobile phone to convey the consent document, and/or an electronic system is used to document consent if documentation of consent is required. When remote consent involves interaction with the research team, such interaction may utilize electronic (e.g., email or text),

audio (e.g., phone) and/or video (e.g., videoconference such as Zoom or Ring Central) modalities.

Electronic Signature (e-Signature): an electronic sound, symbol, or process, attached to or logically associated with an electronic record and used by a person with the intent to sign such record. The Columbia University Electronic Signature Policy https://universitypolicies.columbia.edu/content/electronic-signature-policy establishes requirements for use of an electronic signature in lieu of handwritten signatures for official University activities.

B. Requirements

1. E-Consent. The following requirements are expected to be met for all e-Consenting:

- All elements of informed consent required by DHHS and/or the FDA**,** as applicable, must be included, unless specifically waived.
- When consent information is presented in an electronic format, the e-Consenting system should be easy to navigate, allowing the user to proceed forward and backward in the document and to stop and continue later.
- For Remote Consent that does not initially involve a consent discussion, information should be provided to the potential participant with respect to how questions may be asked (e.g., email sent to the researcher) and answered prior to e-signature.
- Individuals obtaining e-Consent or answering questions for Remote Consent must be appropriately delegated and trained.
- Each e-Consenting mechanism should provide for the generation of a copy of the informed consent form signed by the participant that can be accessed by the participant (e.g., PDF document printable from a website or mailed paper copy)
- When information is presented or consent is documented in an electronic format, the e-Consenting process should incorporate procedures to ensure that electronic documents can be archived appropriately and that all versions of the IRB-approved e-Consent form and all signed e-Consent forms can be accessed and retrieved easily, either by the research subject, as applicable, or a monitor or auditor.
- HIPAA authorization may be obtained electronically, either separately or as part of the e-Consent form. If separate, a copy of the HIPAA Authorization Form must be provided to the research subject and all of the above e-Consent requirements must be consistent with such authorization.

2. E-Signature. The following requirements are expected to be met for all e-Signatures:

- The e-Signature must be linked to the person signing the e-Consent document. This can be done through the use of any of the following:
  - Visually witnessing the signature either in person or using a video conferencing service (e.g., Zoom, Facetime or Skype) and documenting this in the research notes or, with the agreement of the research subject, by recording the session
  - Using security questions, separate individual verification or a double identification system

- Providing to the research subject a personalized link to the document.
- The date and time of the signing must be captured and stored.
- Clicking an "I agree" icon, hyperlink or other similar method to consent to participate in a study, when an identifier is not linked to that action, is not considered to be an acceptable e-Signature.
- When necessary, e.g., to fulfill General Data Protection Regulation (**GDPR**) requirements, research subjects may be asked to show their identification documentation during a videoconference. Scanning or photographing of identification documents should occur only when it would be required in an in-person consent process.

3. Additional University Requirements

- **IRB Requirements.** A request to use e-Consenting in a study must be submitted to and approved by the IRB prior to its implementation. In the protocol, the investigator should:

  - Include a description of the e-Consenting process, the e-Consenting system or software to be used, all ancillary information that will be provided to the research subject and the steps that will be taken to safeguard the integrity and confidentiality of relevant data and electronic materials.
  - If Sensitive Data (as defined in the Columbia University Information Security Charter https://universitypolicies.columbia.edu/content/information-security-charter) will be obtained and/or stored in an electronic format, indicate whether an approved Columbia multi-user system or an encrypted endpoint device will be used, and if applicable, the identity of the multi-user system. See the Columbia University Registration and Protection of Systems Policy https://universitypolicies.columbia.edu/content/registration-and-protection-systems-policy and the Columbia University Registration and Protection of Endpoints Policy https://universitypolicies.columbia.edu/content/registration-and-protection-endpoints-policy.
  - If the e-consent document will be sent to the research subject, describe the secure eSignature system e.g., DocuSign, that will be used, or that it will be sent by email. See the Columbia University Email Usage Policy https://universitypolicies.columbia.edu/content/email-usage-policy for requirements that apply to email transmission.
  - If there is a vulnerable population involved, include a description of the way in which the specific vulnerabilities will be addressed.

- **HIPAA Authorization.** When applicable, a HIPAA Authorization or a HIPAA Waiver of Authorization must be approved by the Columbia IRB.

  A HIPAA Business Associate Agreement (**BAA**) or similar agreement may be necessary if Protected Health Information (**PHI**) will be shared with an external entity or system.

IV. FDA Considerations

Use of electronic systems, archiving and retention of consent documentation for FDA-regulated clinical research studies that use electronic records and e-Signatures must meet the requirements of the FDA 21 CFR 11 regulations (the **Part 11 Requirements).** The Part 11 Requirements are outlined inthe FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures-Scope and Application (September 2003) https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application, and include:

- Validation of electronic systems to ensure accuracy and reliability
- Verification of the identity of signatories
- Ability to generate copies of records suitable for inspection by the FDA
- Protection of records
- Use of secure, computer generated, time-stamped audit trails
- Use of checks to ensure that only authorized individuals can use the system
- Ability to determine the validity of the source of data.

See also the FDA June 2017 Draft Guidance: "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers" https://www.fda.gov/media/105557/download and the FDA's March 2018 "Important Information about Digital/Electronic Signatures" https://www.fda.gov/industry/policiesguidance/important-information-about-digitalelectronic-signatures.

V. Available Systems at Columbia to Facilitate e-Consenting

A. DocuSign

DocuSign is a secure cloud service that provides e-Signature technology for the signing of documents and the creation of document signature workflows. DocuSign can streamline the process of getting documents signed and routing documents through a review and approval cycle. See the Columbia DocuSign information at https://cuit.columbia.edu/electronic-signature.

1. **Fees.** There is a fee for use of DocuSign.

2. **Permitted Uses and Limitations on Use.**

- **HIPAA:** Columbia has a BAA with DocuSign, which permits DocuSign to be used when PHI is involved.

- DocuSign may be used when obtaining e-consent for FDA-regulated research so long as the documentation required by 21 CFR Parts 11 and 50 is obtained.

3. **Record Retention.** DocuSign is not a records retention system and all consent forms must be retrieved from the DocuSign site and stored by the investigator in another location, i.e., wherever the investigator stores all other study-related documents.

B. REDCap

REDCap is a secure web application for building and managing online surveys and databases**,** particularly for research studies. There are multiple installations of REDCap systems at Columbia. If a department does not have a REDCap account, the researcher can check with the Irving Institute for Clinical and Translational Research about possible use of its REDCap account.

1. **Fees.** Fees for the use of REDCap vary by installation.

2. **Permitted Uses and Limitations on Use.**

- REDCap may be used to store Sensitive Information if hosted in a RSAM-certified system. If REDCap is not hosted in an RSAM-certified system, there must be an agreement with the host that describes the applicable data security requirements.

- REDCap may be used when obtaining e-consent for FDA-regulated research so long as the documentation required by 21 CFR Parts 11 and 50 is obtained.

3. **Record Retention.** Signed consent and HIPAA Authorization Forms may be retained in REDCap when a project has been configured to do so. When properly configured, REDCap will automatically store such documents so long as the project is not deleted from the system.

C. Qualtrics

Qualtrics is a survey tool that may be used to facilitate informed consent. Columbia University Irving Medical Center **(CUIMC)** has an education and research site license allowing faculty, staff, and students to use the Qualtrics Survey Platform for free. See the CUIMC IT Qualtrics Online Survey Platform information at: CUIMC IT Qualtrics

1. **Fees.** There is no fee for use of Qualtrics.

2. **Permitted Uses and Limitations on Use.**

- If Qualtrics is not hosted in an RSAM-certified system, there must be an agreement with the host that describes the applicable data security requirements.

- Columbia has a BAA with Qualtrics so it may be used if PHI will be involved.

- Qualtrics may be used in obtaining e-consent for FDA-regulated research so long as the documentation required by 21 CFR Parts 11 and 50 is obtained.

3. **Record Retention.** Signed consent and HIPAA Authorization Forms may be retained in Qualtrics when a project has been configured to do so. When properly configured, Qualtrics will automatically store such documents so long as the project is not deleted from the system.