Introduction
The goal of this best practice document is to help researchers conduct the informed consent process virtually and document the subjects informed consent electronically in ways that meet federal, state, and institutional requirements. The virtual and electronic consent processes must contain the Elements of Informed Consent ($45$ CFR 46.116) and comply with the regulatory requirements for Documentation of Informed Consent ($45$ CFR 46.117). The best practices outlined in this document are only for non-FDA (Food and Drug Administration) regulated research.

All consent processes and materials must be approved by the IRB prior to implementation.

Informed Consent Process
The informed consent process is a basic ethical obligation for researchers. Informed consent is more than just obtaining a signature on a form. It is an active process of sharing information between researchers and potential subjects. The exchange of information can occur by various modes of communication including face-to-face contact, postal or email, telephone or internet calls, video, or through a shared drive.

The virtual consent process should include all the key features of an in-person consent process:

- Must be conducted by someone who is listed as involved in the consent process in HawkIRB
- Provide the necessary information about the research for potential subjects to make an informed decision
- The researcher has a mechanism to assess whether potential subjects understand the procedures and risks of the study
- Potential subjects make a voluntary decision to participate in the study, free from coercion or undue influence, and they can choose to withdraw from the study at any time.

There are several alternatives to obtaining informed consent outside of the traditional in-person interaction and signature on a paper Informed Consent Document (ICD).

Waiver of Documentation of Consent
The first alternative is with a waiver of documentation of consent which waives the requirement for researchers to obtain a signed informed consent document from a subject. It does not waive the requirement for using an ICD or conducting an informed consent process. One or more of the following criteria must be met for the IRB to approve a waiver of documentation of consent:

1. The only record linking the subject and the research would be the consent document and the principal risk would be potential harm resulting from a breach of confidentiality. Each subject will be asked whether the subject wants documentation linking the subject with the research, and the subject’s wishes will govern.
2. The research presents **no more than minimal risk** of harm to subjects and involves no procedures for which written consent is normally required outside the consent.

3. The subjects or legally authorized representatives are members of a distinct cultural group or community in which signing forms is not the norm, the research presents no more than minimal risk of harm to subjects, and there is an appropriate alternative mechanism for documenting that informed consent was obtained.

The consent process must contain all the required elements of consent that would normally be included in an Informed Consent Document. The most common examples of a consent process, where documentation of a signature can be waived, include:

- Verbal consent – in person, via telephone, or over a virtual platform
- Use of an information sheet
- Opting to participate by clicking an “I agree” or choosing not to participate by an “I do not agree” option via a survey platform, such as Qualtrics or Amazon Mechanical Turk (MTurk)

**Options for Signing and Obtaining an Informed Consent Document**

There are also a variety of procedures to obtain a subject’s signature on the ICD and to obtain the subject’s signed ICD, when the Consent Process is not conducted in-person. The informed consent process must be described in HawkIRB (Sections VII.D.29/30) and approved by the IRB. Any method utilized by the study team to obtain a signed consent must include two components: 1) receiving the signed ICD from the subject and 2) providing a copy of the ICD to subjects who enroll in the study. If the study involves the use of protected health information (PHI), subjects must receive a signed copy of the ICD.

A subject’s signature can be obtained on the ICD as, a traditional “wet” signature or by digital or electronic means.

- **A “wet” signature** is obtained by using a writing utensil to physically generate a signature on a piece of paper.
- **A “digital” signature** may be obtained via a stylus or finger to represent a signature.
  - When a stylus or signature with a finger is obtained, it must be consistent with a “wet” signature
  - The signature can be verified by viewing Driver’s license, passport, picture id with a signature, etc.
- **An “electronic” signature** is obtained with a product or eSignature service tool (Adobe, DocuSign, REDCap, etc.) where a password or other form of pre-identification is necessary to ensure tracking, privacy, and identity verification.
  - Digital and electronic signatures are approved by UI IRB, and are consistent with State of Iowa law where electronic signature means “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” *(Uniform Electronic Transactions Act HF 2205, State of Iowa)*

The subject can return the signed ICD, and the research team can provide a signed copy of the ICD to the subject via:

- Fax
- Scanned document
- Mail
Criteria for Use of Electronic Consent (eConsent)
The final alternative to consider as a method to obtain appropriate informed consent may be the use of an electronic consent (eConsent) process. The Office of Human Research Protections (OHRP) and the Food and Drug Administration (FDA) have provided joint guidance about documenting consent through electronic methods (Use of Electronic Consent, 2016). Electronic informed consent uses electronic systems or processes with an electronic media format to obtain informed consent. When using an electronic consent process, the electronic system:

- Should be easy to navigate; subjects need to be able to stop or continue the virtual consent at any point.
- Must employ a method to verify the identity of the subject, guardian, and/or the LAR who signs the electronic Informed Consent Document. Possible verification solutions could include, but are not limited to, use of a:
  - unique log in and password
  - unique code
  - security question
- May use interactive electronic-based technology, which may include diagrams, images, graphics, videos, and narration.
- Should be appropriate for the subject population, taking into consideration the subject’s age, language, and comprehension level.
- May include a way to gauge the subjects understanding of the information in the consent (i.e. optional questions).
- Must be able to provide a signed copy of the ICD to the subject.
- May be used to obtain assent from minors (when required) and parental permission from their parent(s) or guardian(s).

There are additional regulatory requirements under the FDA, FERPA, HIPAA and GDPR (General Data Protection Regulations):

- FDA regulated studies must utilize an electronic informed consent tool that meets 21 CFR 11 compliance. The University of Iowa does not currently have a tool meeting these requirements.
- Studies falling under HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulations) also have additional levels of security, privacy, and verification requirements.
- FERPA (Family Educational Rights and Privacy Act) has additional privacy expectations and requires a signature to release student education records.

Identity Verification When Using eSignatures
The IRB needs to consider state and federal regulations when either a digital or electronic signature method is used to ensure the signatures are legally valid within the jurisdiction the consent is signed and the research is conducted. If a digital or electronic signature is not captured through a system that can verify identity (such as REDCap or Qualtrics) the IRB needs to ensure:

- The signature is unique to the subject
- The electronic or digital signature demonstrates the subject’s agreement to participate in the research
The method of obtaining the signature satisfies the regulations applied to the study (e.g. FDA, HIPAA, state law, institutional policy)

Whether the signature can be legitimately verified from the subject participating in the research (i.e. it must be unlikely that any other individual signed the document)

**Note:** For minimal risk studies, that do not involve minors or other vulnerable populations, it may not be necessary to require identity verification.

- "OHRP recognizes that it may not be possible or necessary for all types of research covered by 45 CFR part 46 to verify that the person signing the informed consent is the subject or the subject’s LAR who will be participating in the research study. OHRP encourages investigators to apply a risk-based approach to the consideration of subject identity. For example, social behavioral minimal risk research will not typically warrant such verification. In addition, informed consent may be waived for minimal risk research meeting the requirements at 45 CFR 46.116(d)." (Use of Electronic Informed Consent, 2016)

**Virtual & eSignature Tools Available at UI**

**Virtual Consent Process**

A virtual consent process is conducted, and ICDs are accessed, stored, and/or shared, via electronic devices through a shared network or over the internet. Zoom and Skype are web conferencing tools that have the capability for video conferencing, as well as just audio to accommodate people who do not have web cameras.

UI Information Technology Services (ITS) has only approved Skype for Business for research involving data protected by the HIPAA Privacy Act.

**Setting up Zoom**

Faculty, staff, and students have access to a Zoom account through the University of Iowa. Potential subjects are not required to have a Zoom account to answer calls or join videos. Zoom calls/meetings can be conducted on all mobile devices, tablets, laptops, and desktop computers.

**Schedule a Zoom meeting/call**

- If you have Zoom installed in Outlook, you can schedule a Zoom meeting through Outlook.
- If you do not have Zoom installed in Outlook, you can schedule a Zoom meeting through the Zoom website.

**Provide Zoom information to potential subjects**

If potential subjects will use Zoom on a mobile device, they will need to download the application on their phone. The Zoom app is compatible with Android devices and iPhones. Zoom is compatible with all Windows and Mac computers.

**Test Zoom Audio & Video Prior to Meeting**

It is best practice to test your audio and/or video system prior to a call/virtual meeting. This will help save time for you and potential subjects.

**Setting up Skype for Business**

All faculty, staff, and students have access to a version of Skype for Business (SfB). There are 2 versions of SfB – licensed and free basic. Unlike Zoom, the fully provisioned licensed version of SfB is not globally available to all faculty, staff, and students. The licensed version must be purchased by individual departments.

- The licensed version of SfB is not available on Mac computers.
• If researchers only have the basic version of SfB they will not be able to call, create video meetings, or share screens, to conduct the eConsent process, with subjects who are outside their system.
  
  o Note: UI Health Care and UI campus are considered different systems for Skype for Business purposes
    ▪ For example, a UIHC researcher with the free basic version of SfB cannot call, create video meetings, or share screens, with someone on UI campus, and vice versa.

• A researcher with a fully provisioned program, can add a subject as a presenter, which then gives them screen sharing capability when using a device/program that supports screen sharing (see Figure 1).

SfB meetings/calls can be conducted on all mobile devices, tablets, laptops, and desktop computers. Potential subjects are not required to have an SfB account to answer calls or join videos. If potential subjects do not have an SfB account, the research team needs to set up a guest account. The guest account will allow subjects to access video meetings. This figure below delineates which SfB features are available on each device.

*Figure 1: Skype for Business: Device Functions & App Capabilities*

```
<table>
<thead>
<tr>
<th></th>
<th>Join Meetings</th>
<th>Share Desktop</th>
<th>Share Program</th>
<th>Presenter Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype for Business Mobile</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Skype for Business Windows</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Skype for Business Mac</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Skype for Business Web App</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
```

*Schedule a Skype for Business meeting/call*

The only way you can schedule an SfB meeting is through the Outlook calendar.

*Downloading Skype for Business information for potential subjects*

If potential subjects will use SfB on a mobile device, they will need to download the application on their device. For potential subjects with an SfB account, they should log into the app with their Office 365 username and password. The app is compatible with Apple and Android devices. For potential subjects who do not have an SfB account, there is a different log in process for Apple and Android devices.

*Joining a Skype for Business meeting*

The way subjects will join a SfB meeting, and the functions available during the meeting, depend on whether they have an SfB account and the type of device they have. The following links provide information about how to join SfB meetings on a variety of platforms.

• A guest joining through the Web App on a desktop/laptop computer
• iPhone
• Android

*Test Audio & Video Prior to Meeting*

It is best practice to test your audio and/or video system prior to a call/virtual meeting. This will help save time for you and potential subjects.
Electronic Documentation Process
Documentation of electronic consent using REDCap meets HIPAA compliance requirements. It is important to remember that HIPAA compliant technology may not be FDA Part 11 compliant for FDA regulated studies. Any electronic informed consent process requires verification of a subject’s identity prior to utilizing electronic means. **None of the electronic tools outlined below can currently be used for FDA regulated studies.**

**REDCap**
REDCap is available as an eConsent tool to conduct HIPAA & non-FDA regulated research. REDCap is supported and managed by the Institute for Clinical and Translational Science (ICTS). Researchers can use REDCap on tablets, mobile phones, and laptop/desktop computers. Use of REDCap requires the setup of an electronic consent document prior to use. REDCap allows individual access with a unique id and password on a per subject basis to assist with subject signature authentication.

**Qualtrics**
Researchers may use Qualtrics for non-FDA regulated studies, and studies that do not use HIPAA data. Qualtrics surveys can be created to include password protected ICD with the ability to capture electronic signatures. If the consent process occurs over the phone, or through Zoom/SfB, once the subject’s identity is verified, the research team member provides each potential subject with a unique password to access the Qualtrics survey. The unique password should be retained as part of the documentation of the subject’s identity. Subjects will then electronically sign the ICD with their fingers, using a touch pad, or by using a mouse.

**HawkIRB Requirements for eConsent Documentation**
All consent processes and documentation methods must be described in HawkIRB exactly as they will be implemented. The HawkIRB sections listed below, though not exhaustive, highlight the most likely sections that need to address the eConsent process and documentation procedures.

Table 1: HawkIRB Requirements for eConsent Documentation

<table>
<thead>
<tr>
<th>HawkIRB Section</th>
<th>eConsent Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VII.D.8</td>
<td>Answer “yes” if the consent process will be conducted through a video meeting over Zoom/SfB.</td>
</tr>
<tr>
<td>VII.D.9</td>
<td>Describe that the consent process is conducted through a video meeting over the internet, at a location of convenience for the subject.</td>
</tr>
<tr>
<td>VII.D.10</td>
<td>Answer “yes” if the consent process will be conducted through an audio only call over Zoom/SfB.</td>
</tr>
<tr>
<td>VII.D.29</td>
<td>Describe the eConsent process and documentation procedures in detail.</td>
</tr>
<tr>
<td>VII.D.30</td>
<td>Describe the eConsent process and documentation procedures in detail.</td>
</tr>
<tr>
<td>X.4</td>
<td>List the electronic systems used in the eConsent process &amp; documentation procedures. Describe the security methods employed.</td>
</tr>
<tr>
<td></td>
<td>- If Zoom will be used to meet with/record minors, be sure to describe the IT security requirements as outlined in the Data Security Guidance document, on the Human Subjects Office (HSO) website.</td>
</tr>
</tbody>
</table>
Privacy and Confidentiality Resources
The Consent process and documentation procedures should follow best practices for collecting, storing, and transmitting Human Subjects data. The Data Security Guidance document, on the Human Subjects Office (HSO) website, provides detailed information about privacy and confidentiality protections, data classifications, and electronic storage & transfer tools.

Privacy and Confidentiality are often used interchangeably, but for IRB purposes, they are distinct concepts. Privacy measures protect the person at the point of data collection and confidentiality measures protect data when it is stored and transferred.

Privacy protections concerning the Consent process can be addressed by:
- Ensuring researchers are in a private location when they conduct the Consent process.
- Reminding subjects to check privacy settings on their computers and mobile devices.
- Reminding subjects to join a call/meeting in a place where they can be alone.

Confidentiality protections concerning documenting and transferring Consent can be addressed by:
- Ensuring researchers understanding how the data they are collecting, storing, and transmitting are classified by ITS.

Ensuring researchers understand that data classification affects which electronic tools are available to use in their studies.