

Division of AIDS (DAIDS) Site Clinical Operations and Research Essentials (SCORE) Manual Appendix:

Clinical Research Site Guidance for Developing an Age and Identity Verification Standard Operating Procedure

Clinical Research Sites (CRSs) must have an Age and Identity Verification Standard Operating Procedure (SOP) in place as detailed in the Age and Identity Verification section of this manual. The following guidance is intended to help CRS staff in developing the SOP.

Each Standard Operating Procedure should describe the following:

- Define how the CRS will implement the procedure for already enrolled participants and new enrollees in ongoing protocols, as well as how to implement this for new protocols.
- Steps that staff follow to establish the participants' age and identity before the person participates in the study. Include any differences in processes for specific populations (e.g. children, transgender, refugees, homeless persons, pregnant women)
- Steps that CRS staff follow to verify the consistency of participants' identity at all subsequent visits throughout the study. The CRS may use the same method for initial verification or establishment of identity and confirmation of identity at subsequent visits, or may establish an alternate method, such as creating a site identification (ID)/biometric ID, or taking a photograph (with date) of the participant for site files. Another possibility could be using a thumbprint instead of signature for illiterate participants. The process should be described as well as how the participant's personally identifiable information (PII) associated with any alternate ID method is protected.
- Which CRS staff members (by role) will conduct the age and identity determination and verification procedure and where/how CRS staff will document the information obtained
- Which forms of ID are acceptable to the CRS to verify participant identification at initial and subsequent visits, and how this is documented in the participants' research records. Include details on the storage and maintenance of any copies of the participant's ID (e.g., in what format will the copy be retained and where the copy is stored), if keeping a copy of the participant's ID is allowable under country and local laws.
- The type of PII elements that are used to verify the participants' identity (e.g., ID number, date of birth [DOB], age, photo, address, biometric measure), and how those PII elements are documented in the research record, and any additional steps that are implemented to maintain participant confidentiality and privacy.
- When automated, or when electronic age and identity verification processes are used, the alternate procedure to follow in case of temporary unavailability (e.g., power outage, no internet access, etc.).

- Sites should also describe what rules will apply if potential participants do not meet the requirements laid out in the SOP. Are there alternative methods available and acceptable to the site and the Institutional Review Board (IRB)/ Ethics Committee (EC), or will participants be turned away?

Additional topics to consider and address in the Standard Operating Procedure:

- Challenges encountered or expected with verifying identity in vulnerable populations (e.g., sex/gender minorities, refugees, homeless persons) at the CRS and alternate procedures that are implemented to verify participant identity in these populations.
- How widely available certain types of ID are within the country/area of the CRS.
- How often IDs must be renewed. If IDs never expire, consider whether an older photo ID of the participant that does not reflect the participants' current appearance is acceptable.
- If ID numbers are unique within the country/region, and if the ID numbers are tracked centrally within the country/region to prevent duplicates.
- If expired IDs are accepted as a form of identification and any relevant grace period permitted prior to renewal for such IDs while taking into consideration specific local conditions.

Examples and Suggestions

Below are examples of identification documents that could be considered by each CRS in developing the Age and Identity Verification SOP at the site. The CRS SOP should describe any specific documents used at the CRS.

Official government IDs with photo, legal name, DOB

- National ID (from any country)
- Passport
- Driver's License/Permit
- State ID (U.S.)
- Military ID
- Waiting Card (applied for National ID, but not yet received)
- Established national biometric system
- Local Council Letter with participant's legal name, photo and DOB

IDs with photo, legal name, but no DOB

- Voter ID Card w/photo
- School ID
- Employer ID
- Local/community government ID
- Credit card with photo

Documents with legal name, DOB, but no photo

- Health passport
- Health/medical records
- Birth Certificate
- Baptismal Certificate (with DOB)

Documents with name, but no DOB or photo

- Documentation of Preferred or Social Name.

Sites can choose to have different processes for initial and subsequent identity verification.

Below are examples of processes that could be used:

- Checking the same forms of ID at initial and subsequent visits
- Setting up a site-created photo/ID at initial visit and checking again at subsequent visits
- Setting up a biometric ID (e.g., fingerprint scan, iris scan) at initial visit and checking again at subsequent visits
- Taking a photo of participant (with their permission) at initial verification for reference at subsequent visits
- Allowing staff knowledge of participant identity
- Allowing participant self-report if allowed by the IRB/EC