UK College of Medicine
Office of Research

Standard Operating Procedure for the COLLEGE OF MEDICINE

Research Documentation – New Study Checklist

Date	Version	Summary of Edits
03.08.2024	1.0	Created SOP using newly updated New Study Checklist
05.10.2024	2.0	Updated language in scope and procedure

Section 1. Background

Regulatory requirements for clinical trials and other forms of clinical research are complex, and non-compliance can negatively impact study participants, investigators, the College of Medicine, and the University. It can be challenging to identify the steps needed or the resources available to ensure compliance. The College of Medicine developed a New Study Checklist as a tool to support study compliance by compiling the various requirements and associated resources into one document. Accurate and complete documentation is the cornerstone of Good Clinical Practice (GCP).

Section 2. Departmental Responsibilities

The Principal Investigator (PI) is responsible for maintaining all required documentation for clinical studies conducted. This checklist can be used by the PI and members of the clinical research team involved in facilitating any of the study start-up activities necessary to activate a new trial.

Section 3. Scope

This checklist should be used as a resource by investigators and their research teams to initiate all clinical studies conducted in the College of Medicine. This checklist describes the process starting from the time the Investigator decides to pursue a potential research opportunity and ending when the trial is activated and ready to enroll. It includes links to helpful resources.

Section 4. Procedure

1. All clinical research teams working with the CRSO to build a new research study in OnCore will receive the New Study Checklist as part of the study submission and review process; however, you do not need to wait for the CRSO to provide you with the

checklist to get started. A current copy can be obtained from the Office of Research by emailing medicineresearch@uky.edu.

2. The New Study Checklist is a resource for investigators and their research teams to ensure regulatory compliance when initiating any clinical study. The checklist should be used cooperatively with any departmental processes to ensure all study start-up requirements are met.
3. Some fields may not apply to your study. Completion of the date received and/or date completed is recommended for study tracking purposes.
4. It may be helpful to retain a copy of the completed checklist by uploading it to OnCore > Documents Section > CoM New Study Checklist.

Section 5. Glossary

Business Associate Agreement (BAA): An agreement between a Covered Entity and its Business Associate under HIPAA. BAAs are required when UKHC (or another covered component of UK) is having someone not a member of its workforce perform services for UKHC where PHI is required to perform the services. For example, if the Sponsor/CRO or a non-employed investigator is providing services to UK/the PI to help de-identify PHI or create a Limited Data Set for the research, then a BAA would be needed. The UKHC Privacy Office makes the ultimate decision as to whether a BAA is needed in any instance, and the EVPHA or one of their delegates signs the BAA. Because certain parts of UK are not subject to HIPAA under our Hybrid Entity Policy and because an entity cannot have a BAA with itself, transfers of PHI outside the covered components of UK's Hybrid Entity (even to another UK department) will likely require a HIPAA authorization (see UKHC's Hybrid Entity Policy, A06-195). Log into the Loop to access UKHC Policy A06-195.

Confidential Information: Any information that the holder or discloser of information does not want to be made potentially freely available to other people. The nature and content of the information that is confidential may be specifically stated in a confidentiality agreement (sometimes called a confidential disclosure agreement (CDA) or a non-disclosure agreement (NDA)) or some other form of agreement that contains confidentiality terms. Also, it may not be defined by an agreement but by law or by some other accepted standard, and further, it may solely be considered confidential in the mind of the holder or discloser of the information. CDAs/NDAs for research purposes are drafted, negotiated, and signed by UK Innovate / the Office of Technology Commercialization for all confidential information coming in and out of the University of Kentucky.

Data Use Agreement (DUA): Allows for data to be transferred from one person or entity to another person or entity. A DUA provides assurances from the receiver of the data to the discloser that the receiver will only use the data for specific purposes and will not be disclosed by the receiver beyond the allowances stated in the DUA. DUAs can also be used to share de-identified data, a HIPAA Limited Data Set (LDS), or non-human related data, and they identify who owns the data and the limited use the receiver can make of the data. If a HIPAA LDS is being shared via the DUA, the DUA also contains provisions that require HIPAA to be followed. The DUA, which must be accepted and signed by authorized representatives of the parties prior to the data being shared, should outline the following: (a) allowable uses and disclosures; (b) approved recipients and users of the data; (c) an agreement that the data will not be used to contact individuals or re-identify them; (d) require safeguards to be implemented to ensure the confidentiality of data and prevent prohibited uses and disclosures; (d) state the discovery of improper uses and disclosures must be reported back to the entity that is providing the data; (e) state that any subcontractors who are required to access or use the data also enter into a data use agreement and agree to comply with its requirements**;** (f) only convey the minimum necessary amount of data for the purpose for which it is disclosed. Research-related DUAs are drafted, negotiated, and signed by UK Innovate / the Office of Technology Commercialization for all data coming in and out of the University of Kentucky.

De-identified: For HIPAA purposes means there is no reasonable basis to believe that the PHI can be used to identify an individual. The ONLY two ways to de-identify PHI are where (a) eighteen (18) different identifiers of the individual and/or of relatives, employers, or household members of the individual are completely removed from the data (these include not just name but also any dates, excepting year, associated with them [including without limitation: birth date; admission date; discharge date; date of death; dates of other health events or services, etc.]) AND UK does not have actual knowledge that the purported de-identified information could be used, alone or in combination with other information, to identify the individual; or (b) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, using those principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information, and that experienced person documents the methods and results of the analysis that justify such determination. For (b), it takes extraordinary circumstances to achieve this form of de-identification (to the point that only two statisticians in the US are consistently asked to do this work), and if the PHI that has been purportedly de-identified originated at the University of Kentucky, verification of this de-identification would likely require separate confirmation. For more information on de-identification in the HIPAA context, see CFR 45 CFR Part 164 Subpart E -- Privacy of Individually Identifiable Health Information (review sections a-c) [https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E#164.514] and Guidance on De-identification of Protected Health Information (hhs.gov) [https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf]

Limited Data Set (LDS): For HIPAA purposes is a subset of PHI (not all PHI) that HIPAA permits to be shared with certain entities for research purposes, public health activities, and healthcare operations without obtaining prior authorization from the individual, if certain conditions are met. In contrast to de-identified PHI (which is no longer classified as PHI under HIPAA once de-identified), a limited data set under HIPAA is still identifiable protected information and subject to HIPAA requirements. However, a HIPAA limited data set can only be shared with entities that have signed a data use agreement with the entity providing that limited data set. For more information on LDS, see 45 CFR Part 164 Subpart E -- Privacy of Individually Identifiable Health Information (review section e) [https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E#164.514].

Material Transfer Agreement (MTA): An agreement that governs the transfer of tangible research materials between two organizations. The materials could include specimens, cell lines, mice, plants, equipment, testing supplies, etc. MTAs describe the terms for exchanging the material and how the material can be used by the receiving party. MTAs are drafted, negotiated, and signed by UK Innovate / the Office of Technology Commercialization for all material coming in and out of the University of Kentucky.

Personally Identifiable Information (PII): Any information about an individual that either (a) can be used to distinguish or trace their identity, such as name, social security number, date and place of birth, mother‘s maiden name, biometric records, etc., or (b) is linked or linkable to an individual, such as medical, educational, financial, and employment information. See National Institute of Standards and Technology (NIST). NOTE: The U.S. government has stated that “the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.” See Government Services Administration (GSA). Please also note that the Commonwealth of Kentucky has a law governing data breach notification requirements applicable to public agencies, which includes public universities such as the University of Kentucky and certain other parties, and that law includes a separate definition for “Personal information” that is different than PII and PHI (defined below). See https://apps.legislature.ky.gov/law/statutes/statute.aspx?id=43575 (review section 6) for that definition.

Protected Health Information (PHI): Health data (including demographic data) created or received by employers, HIPAA-covered entities (entities directly regulated by HIPAA—which includes health care providers that conduct electronic transactions under HIPAA, including UK HealthCare, and certain other entities), and Business Associates (a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity), that relates to the past, present or future health condition of or provision of health care to an individual and that either identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.