E-IRB Operations

Table of Contents

General Description

The E-IRB system is an in-house customized web-based program aimed at facilitating review and approval of research proposals from a human subject protections perspective in accord with the Common Rule and applicable Food and Drug Administration (FDA) regulations (see other IRB/ORI policies and SOPs). Within this secure online system, E-IRB facilitates Institutional Review Board (IRB) application submissions and IRB recordkeeping by the researcher; processing, tracking, and recordkeeping by Office of Research Integrity (ORI) staff; and review and documentation of determinations by IRB members.

The core records contained in E-IRB include but are not limited to:

- the IRB application and relevant attachments;
- correspondence between the researcher, ORI, and the IRB, pertinent to the application and review;
- documentation regarding events related to conduct of the research (e.g., Protocol Violation);
- IRB letters (e.g., approval letter);
- reviewer documentation;
- meeting agendas.

Meeting minutes are maintained external to E-IRB, as are research participant records and other regulatory documentation not directly IRB related.

User Information

The following provides a description of various key E-IRB users.

Research Information Services (RIS)

The University of Kentucky department that devoted a team of programmers responsible for E-IRB design, development of programming, and implementation of code.

RIS maintains server security and integrity; system upgrades; and follows the University's Administrative Regulations for 10:7 – Security of Data and 10:8 – Security of Information Technology Resources.

E-IRB System Administrator

A "system administrator" position held within the Office of Research Integrity delegated to (including but not limited to):

- access back-end features restricted to the administrator role;
- facilitate further design and development of features;
- ensure the E-IRB system continues to function appropriately;
- manage the discovery of issues and bugs (via user feedback and review of the system's web based error log);
- train and educate end-users;
- update IRB reviewer documentation in the database (as deemed appropriate with proper concurrence from the corresponding reviewer), and,
- submit Linkblue account requests to campus IT.

Office of Research Integrity (ORI) Staff

Employees of the Office of Research Integrity who are responsible for facilitating all aspects of review and approval of human research. For more detail, see "About ORI" on ORI's home web page.

RIS and the ORI E-IRB System Administrator control who is given access to the E-IRB system in an ORI role.

The ORI role permits a user to (including but not limited to):

- access the E-IRB database;
- access submitted, approved and inactive applications and each one's history including IRB determinations and Quality Improvement materials;
- insert comments and view PI, ORI and IRB comments about the submission;
- insert and view additional protocol-specific data in the "ORI Flags" tool;
- route applications to the PI and the IRB;
- select IRB meeting dates and adjust agendas;
- select IRB reviewers;
- change protocol process type (Full to Expedited and vice versa) and IRB teams;
- generate IRB correspondence;
- manage and view human subject protection (HSP) training records and
- retain other documentation pertinent to the research application.

ORI staff also have the capability to edit an application on behalf of the researcher. At the discretion of ORI staff, edits may be made to the application, but it is only generally accepted to do so with permission from the researcher in writing.

Institutional Review Board (IRB) Member

Individual appointed by the Vice President for Research to provide reviews of proposed research activities. For more detail, see the "Nuts and Bolts of IRB Membership" section on the IRB Membership web page, as well as the IRB Membership SOP [PDF].

RIS and the ORI E-IRB System Administrator control who is given access to the E-IRB system in an IRB role.

The IRB role permits a user to (including but not limited to):

- access the E-IRB database;
- access submitted and approved applications and each one's history including determinations and Quality Improvement materials;
- insert comments and view PI, ORI and IRB comments about the submission;
- review agendas;
- and complete assigned "IRB Review" tasks.

The application is in read-only view for IRB members. A submission for which IRB review has been completed can only be routed to ORI.

As established by this policy/guidance document and federal regulations, there is no requirement for a UK Institutional Review Board (IRB) Chair/designee to hand-sign or e-sign approval letters; the security of the Linkblue process suffices to validate determinations. Documents generated electronically within E-IRB as a result of IRB review are clearly identified by Document Type and are secured in the E-IRB system.

Consultant

A non-IRB member, with expertise not otherwise held by an IRB member, who is chosen by ORI staff to provide review for appropriateness of a research proposal (e.g., Cultural consultant).

Consultants access the E-IRB system in the Researcher role, and click on the "Consultant Reviews" tab on his/her Dashboard to see assigned reviews. A consultant's access to an application is equivalent to IRB role (but consultants do not get IRB role so they don't have access to entire IRB database), as is the "IRB Review" task button.

Auditor

An individual charged with reviewing some aspect of UK's human research protection program and who should have limited access to the E-IRB system to perform his/her auditing responsibilities (E.g., AAHRPP site visitor).

RIS and the ORI E-IRB System Administrator control who is given access to the E-IRB system in an "Auditor" role. For non-UK individuals, a Linkblue account is established prior to the auditor's arrival.

The "Auditor" role permits a user to (including but not limited to):

- access approved applications in read-only view by protocol number;
- view PI, ORI, and IRB comments about the submission;
- access protocol history of approved applications including IRB determinations and Quality Improvement materials.

Principal Investigator (PI)/Researcher

An individual engaging in human research activity. The default role assigned to an individual logging into E-IRB is the "Researcher" role unless the user has been designated an additional role (e.g., IRB role) by RIS or the ORI E-IRB System Administrator. There are different levels of access offered within the researcher role.

It is IRB policy that the Principal Investigator (PI), identified as such in the PI Contact Information section of an E-IRB application, holds primary responsibility on the research project and is the only individual with permissions to sign the PI Assurance Statement. The PI is authorized to create, edit, and submit an initial review (IR) application, continuation review (CR) application, final review (FR) application, or a modification request (MR) application as well as "Other Reviews" (Unanticipated Problems (UPs) involving risk to subjects or others; Protocol Violations (PVs); Deviation/Exception requests (DEV/EXC); and, if certain circumstances are met, an Administrative Study Closure (IRB review for this kind of "Other Review" is not required)).

Additionally, having a designation of PI permits the user to (this is not an all-inclusive list):

- access submitted, approved, and inactive applications and each one's history;
- create a record for Non-UK Personnel;
- insert comments* and view PI and ORI comments about the submission (*comments feature is not available on a *draft* application).

"Role for E-IRB access" – the user's selection will determine what kind of access the researcher will have to the E-IRB application created:

Editor ("DP" role) - individuals given edit authorization have all the capabilities as the PI for creating, editing, and submitting (applications and Other Reviews), with the exceptions of submitting an administrative study closure and signing the PI Assurance Statement. Per the PI's Assurance Statement, when the DP submits on behalf of the PI, it is with the understanding that the PI has reviewed the materials for accuracy.

Reader ("SP" role) - individuals assigned the "SP" role can view the currently approved application in read-only mode, and access protocol history.

"Is Contact" – regardless of access assignment (DP or SP), individuals designated as a contact will, in addition to the PI, receive notifications about the application (e.g., requests for minor revisions, Continuation Review requests, etc.).

Department Authorization (DA) or other Designated Signee

An individual serving in a leadership role to the PI and who has been assigned to complete an Assurance Statement for the proposed research per IRB policy. This responsibility typically falls on the shoulders of the PI's Department Chair and therefore the role of such a person has been dubbed "Department Authorization" (DA), although someone serving in an equivalent position could serve as DA.

Other "Designated Signees" - Under IRB policy, an Assurance Statement is also required from the PI's Faculty Advisor if the PI is a UK student. A third signee role is available for PI's who need to send the application for "Review by Other" per his/her department policy.

In the *Signatures (Assurances)* section of the E-IRB application the researcher identifies the individual(s) (e.g., Department Chairperson, Faculty Advisor, Other) within his/her unit responsible for completing an assurance statement. For additional details on the IRB policy governing this process, see the ORI guidance document, "What does the Department Chairperson's Assurance Statement on the IRB application mean?" [PDF]. Once an assignment to complete an Assurance Statement has been saved in the *Signatures (Assurances)* section and the application has been "sent for signatures," the assigned individual has access to the E-IRB application for review and is required to "sign" the assurance statement (using Linkblue ID and password) before the PI's application is eligible for submission to the IRB.

Should a Signee require changes to the application prior to signing, communication with the PI in that regard needs to occur external to the system; the PI has access to edit the application while it awaits Assurance signatures.

Business Rules

(not an all inclusive list)

Comments on Application and Review Notes on Other Reviews (C & RN)

Only ORI staff can select the audience for each C & RN inserted: PI-only; IRB-only; or both PI and IRB.

- The PI/researcher role can only see researcher and ORI's C & RN.
- IRB role and Auditor role can only see researcher C & RN and C & RN inserted by ORI where IRB is the audience.
- ORI role can see all C & RN.

Comments and Review Notes can be re-viewed in an application's Protocol History in accord with the rules described above.
Tip: be aware of which role you are in when viewing an application.

Attachments

Document Type of an attachment dictates which users can access and upload the attachment, and whether the document is available from the time of attachment on, or only to the phase to which it was attached. Special attachments rules are listed below, otherwise, the attachment is available to all users.

- ORI Documentation/ORI Doc - attached to applicable phase for users in ORI role;
- Miscellaneous IRB Documentation (IRB Doc) - attached to applicable phase for users in ORI role, IRB role, and Auditor role;
- QI Documentation (QI Doc) - available from the time of attachment on for users in ORI role, IRB role, and Auditor role;
- COI Management Plan – available from the time of attachment on for users in ORI role, IRB role, Auditor role, and users accessing the protocol via the OSPA group Dashboard.

ORI Flags

Only ORI can see and edit the entire contents of ORI Flags; all edited fields and attachments are reflected on the phase of the application to which they were added, unless otherwise specified in ORI Flags (e.g., When "ORI Notes" and COI Management Plans are added, they will be available on the current phase and then carried forward to the next phase of the application).

Applications accessed through the OSPA group ("External") Dashboard permit the user to see the SFI section and ORI Flags History.

Group Dashboards ("External" role)

Group Dashboards were created to enable select individuals logged into E-IRB to acquire information and materials from submissions that fall under the applicable unit's purview, without giving access to the entire IRB database.

The ORI E-IRB System Administrator (and RIS) controls who is given access to specific group Dashboards; the group Dashboard is in addition to the default Researcher Dashboard.

E-IRB automatically flags applications to fit into specific groups based on established criteria for Markey Cancer Center (MCC); Office of Sponsored Projects Administration (OSPA); the Center for Clinical and Translational Sciences (CCTS); and COVID-related research. Each group's Dashboard only lists applications that meet the criteria for that group.

E.g., MCC representatives have the option to toggle from their Researcher Dashboard to a Dashboard (under "External" role) that displays approved applications involving only cancer research; CCTS representatives have the option to toggle from their Researcher Dashboard to a Dashboard that displays only approved applications that are clinical trials and/or clinical research.

Individuals with an assignment to a specific group dashboard will be able to click on the IRB number in that group and:

- access applications in read-only view;
- view PI and ORI comments about the submission; and

- access protocol history of approved applications including attachments, completed Other Reviews, All Events, and Cancelled Submissions.

Compliance

The E-IRB system was designed to facilitate enforcement of University of Kentucky (UK) policies governing access to and use of technology resources and electronic signatures, as well as federally mandated requirements in three areas as described here: Electronic Signatures, Record Archiving (Audit Trail), and Security Controls.

Electronic Signatures

The University of Kentucky Information Technology Services (ITS) created the term "Linkblue" to define a directory account (a unique user id and password) which can be used by employees and students to securely connect to many campus-wide systems. Users of the E-IRB system apply the term Linkblue as the equivalent to “electronic signatures,” with the understanding that the Linkblue ID and password is the legal equivalent of a personal handwritten signature. When a user accesses E-IRB with his/her Linkblue, all actions performed thereafter are considered to be taken by the individual associated with that Linkblue account.

Linkblue accounts are meant to be used according to University of Kentucky (UK) policy (Administrative Regulation (AR) 10:1 – Use of Technology Resources; 10:5 – Electronic Signatures Policies and Procedures), with the intent of meeting the Food and Drug Administration’s (FDA) regulatory requirements set forth in 21 CFR Part 11.

Employees applying an electronic signature on documents attached to E-IRB applications are expected to abide by UK policy and guidance as set forth in Administrative Regulation (AR) 10:5 and Business Procedure Q-1-6 outlining the University’s policies on e-signatures.

Audit Trail

Record archiving is facilitated by the comprehensive logging of every action taken within the E-IRB system, including changes to existing records. These logs record each action, the identity of the individual performing the action per Linkblue ID, and the action's date and time. To streamline the user’s experience, not every action logged is visible in the E-IRB interface, but can be retrieved upon request.

The researcher must re-enter his or her own unique Linkblue in order to verify identity before performing key functions within the electronic workflow (e.g., a PI Assurance Statement can only be completed by entering the PI’s Linkblue). The signee’s name and date/time the action was completed is recorded under the Signature/Assurances section of the E-IRB application.

Actions permissible only by users in the IRB role (“IRB Review task”) are recorded with the user’s name, and date/time the action was completed under the Protocol History Determinations tab, which is accessible only to individuals assigned the ORI, IRB, or Auditor role. Official IRB correspondence (e.g., PDF letters on letterhead) include all relevant dates in headers or in the body of the document and are issued by ORI only upon documentation of a determination by the IRB.

Security Controls

The E-IRB system addresses the security requirements by including:

- **Controls for identification:** UK maintains identifying information about each employee/student in association with a Linkblue account. The E-IRB system uses Linkblue to verify the individual's identity.
- **System access is limited to authorized individuals:** Every E-IRB user must have an active University of Kentucky Linkblue account with a unique name and password in order to log-in to the E-IRB system. If an individual is no longer affiliated with the University of Kentucky, his/her Linkblue account is deactivated and access to E-IRB will be denied.
- **Individuals are held accountable and responsible for actions initiated under their electronic signatures:** Assurances of compliance by designated signees (e.g., Department Authorization (DA)) are recorded in the E-IRB system. The University of Kentucky follows standard operating procedures for its Quality Improvement Program aimed at identifying issues or verifying compliance with responsibilities delineated to PIs and study personnel on IRB-approved applications.
- **Controls for a closed system:** E-IRB is a closed system (a valid Linkblue account is required for access to the network). UK has written Administrative Regulations (AR) that prohibit employees/students from obtaining or using another's login credentials or otherwise access technology resources to which authorization has not been expressly given (AR10:1; IV.J.c.i.). E-IRB system privileges vary depending on assigned roles (e.g., Researcher, ORI, IRB, Department Authorization (DA)). The Linkblue identifies which predetermined roles a user may hold, and each role controls which responsibilities and permissions a user has. For example, only users authorized in an IRB role can perform IRB actions, and only an individual serving as a Principal Investigator (PI) can sign a PI Assurance Statement. UK maintains all information associated with research proposals and reviews, and this information is governed by UK policies and procedures for data security (Administrative Regulations 10:7 – Security of Data and 10:8 – Security of Information Technology Resources).

System Maintenance

E-IRB IT support (Research Information Services (RIS)) holds shared responsibility with UK campus IT for the disaster recovery plan for data maintained on E-IRB's UK server:

- Backup media is stored in a secure, geographically separate location from the original and isolated from environmental hazards.
- UK uses Tivoli Storage Manager (TSM) for its restore and backup needs.
  Backup/Restores
  - Servers (including shared network drives):
    Backups will be performed daily via campus.
    - Restores will be performed within four (4) business hours.
  - Databases:
    - Backups of production databases will be made both locally and via campus for 30 days according to the following schedule:
  - Locally:
    - 4 weeks daily backups;
    - 4 weekly backups;

- 1 monthly backup;
- 2 weeks of transaction logs

○ Campus:
30 days of daily full SQL backups
- Restores of a complete database will be performed within four (4) business hours. Partial database restores are dependent on data consistency issues and may take significantly longer.

Addressing missing functionality (e.g., bugs) and development of new features in E-IRB is ongoing and prioritized by user feedback received either through the EIRBsupport@uky.edu mailbox or by the E-IRB System Administrator. In coordination with the E-IRB Administrator, RIS implements an average of 10 system updates a year.

Health Insurance Portability and Accountability Act (HIPAA)

Protected health information (PHI) is defined as any of the 18 identifiers listed in the HIPAA Privacy Regulations in combination with health information that is created or maintained by a UK covered entity (CE) department relating to the past, present, or future physical or mental health or conditions of an individual. While the intent of E-IRB is not to specifically collect PHI, it is possible that in the researcher's reporting of events (e.g., Unanticipated Problem involving risk to subject or others) or submissions (e.g., Continuation Review materials), PHI may be inadvertently collected. It is understood that this data may be viewed by ORI staff, IRB members, RIS staff, and/or Auditors within an administrative capacity and not with the intent of being shared or used in any other manner than for quality improvement and/or consideration of IRB approval of the research study.

End User Training

In addition to instructions within the E-IRB application, and guidance documents on the E-IRB web site, online video tutorials are available to ORI staff, researchers, and IRB members to assist with use and navigation of the E-IRB system. Live online training or in-person consultation is available upon request.

ORI staff are periodically provided with training by the E-IRB System Administrator on updates to or issues with the system. ORI also has an internal E-IRB Training Manual focused on features and usage of the system for responsibilities held by ORI staff.

Legacy System Usage

Key data from ORI's legacy system ("ORI database") for Full and Expedited applications was imported by the researcher at Continuation Review time (mandatory as of January 22, 2018) for each study still requiring IRB-approval:

Protocol Type (Medical vs. Nonmedical); Process Type (Full or Expedited); PI Name; Study Title; approval period, and old ORI database protocol number (may be referred to as "Transition #").

Applications certified as exempt prior to June 22, 2017, did not require importing.

E-IRB Operations

For historical reference, the paper records for active studies remain secured in ORI office space in accord with the IRB/ORI Recordkeeping SOP. The “Transition #” is maintained in a field at the top banner of each imported application in E-IRB. The “Transition #” helps identify whether paper records exist to supplement the application in E-IRB.

Office of Research Integrity and Research Information Services
Updated 7/19/23 by Judi Kuhl (Linkblue)
J:\Master Outreach Documents\Survival Handbook\D - Guidance-Policy-Educational\D155-E-IRB Operations.docx