Electronic IRB Submission Process Security and Data Management Statement

The Wake Forest University Health Sciences (WFUHS) Institutional Review Board (IRB) utilizes an electronic submission process (eIRB) for all protocol submissions. All study related documents requiring review by the WFUHS IRB must be attached electronically to the protocol application. Documents must be either Microsoft Word or Adobe PDF format.

Security and data management standards equivalent to those used by Wake Forest University Health Sciences and North Carolina Baptist Hospital (the Medical Center) to maintain the security of all medical and financial information are applied to the eIRB system. The standard for maintaining the physical security and integrity of the data and system, backup and recovery, and user access security are the Medical Center standards applied to all enterprise wide systems.

The application is hosted by two secured servers which operate behind the Medical Center firewall. Access to eIRB therefore requires either physical access to the Medical Center network or remote access via encrypted transmission. The servers are secured through controlled physical access.

Access Controls

- eIRB represents a closed system meaning an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
- Access is limited to authorized individuals. Authorized individuals must have both a Medical Center Account consisting of a user name and password, and have been assigned a role within the eIRB system.
- Access to the eIRB system requires a Medical Center Account (user name and password) which is unique to one individual. An individual without a Medical Center Account or whose Medical Center Account has been disabled can not access the eIRB system. Individuals work only under their own Medical Center Account. The establishment, control and security of Medical Center Accounts are directed by WFUBMC Information Systems.
  - Key Points for the Medical Center Policy
    - The account (user name and password) is unique to one individual such that no two individuals have the same combination of user name for an active account.
    - Individuals are held accountable and responsible for action initiated under their account by the terms of a signed Confidentiality Agreement.
    - The identity of the individual is verified before an account is established.

    - » Controls are followed for loss management procedures to disable compromised accounts.

- The eIRB system uses defined levels of access called user roles to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or out device, alter a record or perform the operation at hand. Individuals using the eIRB system are assigned a specific combination of user roles which define the information an individual can access and his/her ability to create or modify information. User roles are assigned based on the specific function or role an individual plays in the development, conduct or oversight of research projects.
    - Study staff roles (PI, Co-Investigator, Study Coordinator and Other Study Staff Members), IRB Committee Chair roles and IRB Committee Member roles may be assigned by the IRB Administrative Staff, IRB Director, or Executive Director for Research Regulatory Affairs.
    - IRB Administrative roles, Department/Section approver role, ancillary committee approver roles and all other administrative roles may be assigned by the IRB Director or Executive Director for Research Regulatory Affairs
    - IRB Director role is assigned by the Executive Director for Research Regulatory Affairs
    - The role of System Administrator requires the approval of both the Executive Director for Research Regulatory Affairs and the Associate Dean for Academic Computing and Information Services.
- Device access to the eIRB system is limited to devices within the Medical Center Network or by remote access via Citrix Portal or Virtual Private Network. Medical Center Information Systems grants and manages remote access privileges.

<u>Electronic Signature</u>

- Electronic signature mean a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.
- Each electronic signature in eIRB is unique to one individual and is not reused by or reassigned to anyone else.
- Electronic signatures in eIRB employ two distinct identification components, a user name and password.
- Medical Policy and Procedure establishes controls to ensure user name and password security and integrity.
- Executed electronic signatures are linked to their respective electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.
- The signed electronic record contains information associated with the signing that clearly indicates the printed name of the signer; data and time when the signature was executed and the meaning.
- All actions executed by a signing authority are logged.

Audit Trail

- The eIRB system uses a secure, computer-generated date and time-stamped audit trail to automatically record the date and time of operator entries and actions that create, modify, or delete electronic records. Previously recorded information is not obscured by record changes. Audit trail information is retained a least as long as that required for the subject electronic record and is available for review and copying.
- The computer-generated date and time stamp is under the control of the server on which the eIRB application resides. The Windows Time service is used to maintain the date and time on this server. It configures itself by synchronizing with the Windows Time service available on one of the WFUBMC domain controllers. The ability to change the date or time is limited to Academic Computing server administrators. Even if a change in time is made by an administrator, the time will be corrected at the next synchronization.
  - Key points for Academic Computing Policy
    - Access is limited to authorized individual
    - Changes are documented
    - Detected Discrepancies are reported
    - The system is synchronized to the date and time provided by trustee third parties

Validation

- Uses Click Commerce Research Extranet – need brief description of design specification that describes what the software is intended to do and how it is intended to do it
  eIRB refers to the WFUHS implementation of Click Commerce Research Extranet, a web-based application for Research and Healthcare process automation. The base product is built on the Microsoft .Net Framework and utilizes a SQL Server database backend. Click Commerce releases periodic service packs and upgrades in order to improve performance and functionality as well as to stay compliant with new Microsoft technologies as they are released. Click Commerce uses feedback from the Click Compliance Consortium, a consortium of Click Commerce Research Extranet customers, to guide ongoing product development and to beta test new releases of service packs and upgrades.

- Design level validation is maintained by Click Commerce

System Controls

- All changes to the eIRB computerized system, such as software upgrades, security and performance patches, and equipment or component replacement are evaluated and tested to ensure the integrity of the data is maintained.
- All changes to the system are documented.
- All versions of the software are documented.

Contingency Plan

- In the event that the eIRB system is not functional for an extended period of time due to server malfunction, a backup "warm" site will be enabled on a separate server in order to maintain the integrity and continuity of data within the site. This warm site is a fully functional site that can be enabled within a half hour. As a precaution, data from eIRB is copied to the warm site server every 15 minutes.
- In the event the eIRB system is not functional and the outage is anticipated to be 24 hours or less, only protocol activity that is immediately required to address issues related to the safety, rights or welfare of research subjects will be acted on. The determination as to whether an issue needs to be immediately addressed will be made by either the IRB Director or an IRB Chair. Documentation will be made on paper forms made available to the study team by either web posting, FAXing, or in the IRB Office. Following resumption of the system the study team will transfer all paper information to the eIRB system and attached scanned copies of all paper documents.
- In the event the eIRB system is not functional and the outage is anticipated to last greater than 24 hours, the IRB will shift to a paper based system. Documentation will be made on paper forms made available to the study team by either web posting, FAXing, or in the IRB Office. Following resumption of the system the study team will transfer all paper information to the eIRB system and attached scanned copies of all paper documents.
- In the event the eIRB system is not functional and the system can not be restored, active protocols will be identified by querying the user base, querying other Medical Center databases, and contacting sponsoring agencies. Copies of required documents will be requested in order to reconstruct files. The IRB will review each reconstructed study file. The user base will be notified to suspend all study activities except where necessary to ensure the safety, rights or welfare of enrolled subjects until the IRB has reviewed the reconstructed study file. Such a failure will be reported to OHRP, FDA and all other applicable agencies as required by regulation.

Back-up and Recovery

- Backups are performed each day on eIRB servers by Legato. A complete backup is scheduled once a week and incremental backups are scheduled all other days. Legato keeps the last three versions of all files. This backup routine is standard for servers on the MEDCTR network.
- Data is copied from eIRB to the warm site every 15 minutes. This ensures that data in the backup site is never more than 15 minutes removed from data in the live site. The Academic Computing Warm Site Manual details the process of enabling the warm site.

Version Date
4-10-07