06.3 HHS PIA Summary for Posting (Form) / NIH NCI Central Institutional Review Board (CIRB)

PIA SUMMARY AND APPROVAL COMBINED

PIA Summary

Is this a new PIA 2011? No

If this is an existing PIA, please provide a reason for revision: PIA Validation

1. Date of this Submission: 8/24/2012

2. OPDIV Name: NIH

3. Unique Project Identifier (UPI) Number: Requested

4. Privacy Act System of Records (SOR) Number (If response to Q.21 is Yes, a SORN number is required for Q.4): SORN 09-25-0200

5. OMB Information Collection Approval Number: Requested

6. Other Identifying Number(s): NCI Control No. N02CM-2008-00010

7. System Name (Align with system Item name): NIH NCI Central Institutional Review Board (CIRB)

9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed: Mike Montello

10. Provide an overview of the system: The overall purpose of the NCI CIRB data systems is to provide comprehensive informatics support for a centralized process of facilitating Institutional Review Board (IRB) activities for National Cancer Institute (NCI) Cooperative Group clinical trials. The NCI CIRB data systems is comprised of 3 modules and fulfills multiple functions: 1) to enroll local sites with their contacts and track their local IRBs, 2) to manage study-related documents and other information, 3) to convey study and board review information to sites and collect from sites facilitated review acceptance forms via the web, 4) to track and report on CIRB help desk issues, and 5) to track and report on board membership attendance and management of board member reimbursement.

The three modules are comprised of the Membership Attendance and Tracking (MAT) internal database, and CIRB HelpDesk Application internal database (CHAD) maintained by EMMES; the CIRB Enrollment System (CES), CIRB Website hosted by CTIS; and, IRBManager web-based application hosted by BEC.

Information is sent from IRBManager to the CIRB oracle database which serves as the backend of the CIRB website. The MAT and CHAD databases are internal systems used for operations and do not exchange information.

13. Indicate if the system is new or an existing one being modified: Existing

17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system? (Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether

provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?): Yes

21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4): Yes

23. If the system shares or discloses IIF please specify with whom and for what purpose(s): IRB Manager and CIRB Web Site, both of which are modules of the CIRB system, exchange study information and related documents. The CIRB web site includes both password-protected and publicly available sections. Some of the information exchanged is also publicly available elsewhere. This system falls under the guidelines of Privacy Act System of Records Notice 09-25-0200.

30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory: Legislation authority is the Public Health Service Act (42 U.S.C. 241, 242, 248, 282, 284, 285a-j, 285l-q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.), CFR Title 45 Part 46 (Protection of Human Subjects), and CFR Title 21 Part 50 (Protection of Human Subjects) and Part 56 (Institutional Review Boards).

The types of data used are both scientific and administrative and used to inform board members concerning the studies under review, manage the operations and communications of Adult and Pediatric Central Institutional Review Boards, and convey information to sites concerning studies reviewed by the CIRB and decisions made by the CIRB.

The CIRB Operations Office staff routinely generates standard and ad-hoc reports, including quality control metrics that display CIRB information concerning studies, Boards, local sites, local site IRBs, and Operations Office activities.

Personal information provided by Board members is provided as part of their voluntary service to the CIRB and the NCI. Names and contact information provided by contacts at the local sites and IRBs is provided by site representatives on a voluntary basis but required for effective participation of their site in the CIRB Initiative.

31. Please describe in detail any processes in place to: (1) notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) how the information will be used or shared.

(Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]) The CIRB collects IIF from Board members and local sites using forms that may be completed as hard or electronic copies and mailed or emailed to the Operations Office for data entry. Board members and site representatives are aware of the purposes for which their contact information will be used. Privacy statement is available

electronically and additional privacy statement information is shared during enrollment application process.

Changes to CIRB processes, including development, utilization, or revision of CIRB information systems and using or sharing of data, are subject to review and approval by an NCI Project Officer. IT Change Management processes are in place at the respective contractor or subcontractor.

Users that access the systems must reregister on an annual basis and any changes would be communicated through that process.

32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII): Yes

37. Does the website have any information or pages directed at children under the age of thirteen?:

50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):

54. Briefly describe in detail how the IIF will be secured on the system using administrative, technical, and physical controls.: CIRB data is maintained in secure databases.

The following are in place as Management Controls:

- Login Banners
- Rules of Behavior
- System Security Plan
- Configuration Management, Change Management Plans and Processes
- Disaster Recovery Plan

The following are in place as Technical controls for CIRB:

- Network security via User ID and Password login
- User ID and Passwords required to login to CIRB applications
- The CIRB applications are hosted within Network boundaries and protected by Perimeter Firewall and Intrusion Detection
- SSL Encryption is enabled for access to web based interfaces of CIRB modules, where necessary
- Proactive Systems Monitoring and Alerts Management
- Anti-virus, security updates and patching procedures
- Periodic scans for CIRB systems – both internal and external
- Incidence Response Procedures

· System and Database Audit Trails and Logs

The following are in place as Operational controls for CIRB:

· Personnel Security

· Security Clearance Process for designated contractor and subcontractor personnel working on CIRB

· Contractor and Subcontractor Hiring and Termination Process (NIH suitability investigations for key personnel)

· NIH Non-Disclosure Agreement for all contractor and subcontractor employees working on CIRB

· Annual requirement for all employees to take/review NIH CIT Security Awareness Training

· Physical and Environmental Protection (including individualized door entry cards and photo ID)

· Visitor Log Procedures

· Backup Procedures

· Offsite Storage for Tapes

· Video Surveillance of Data Center

· AC Maintenance Process

· Contingency / Disaster Recovery Plan

· Incidence Response Procedures

· Alerts and Scans

· Identification and Authentication

· User Account Management Process

· Role based user access to systems

· Password Change Policies (for systems per NIH requirements)

· Procedures for handling lost/compromised passwords

· Audit Trails

PIA Approval

PIA Reviewer Approval: Promote

PIA Reviewer Name: Suzy Milliard

Sr. Official for Privacy Approval: Promote

Sr. Official for Privacy Name: Karen Plá

Sign-off Date: 9/28/2012

Approved for Web Publishing: Yes

Date Published: <<Date approved for Web Publishing>>
