eProst System Policies & Procedures

Initial Approval Date:	12/07/2010
Revision Date:	02/25/2011

Introduction

eProst ["Electronic Protocol Submission and Tracking"] is the Human Subject Research Office's (HSRO) web-based, computer system that automates the entire lifecycle of human subject research activity.

eProst is designed to support both behavioral and biomedical research studies, including studies requiring IRB approval by the full panel or those that require expedited or exempt review.

Through eProst, human subject research studies may be:

1) written and submitted to the University of Miami's Institutional Review Board (IRB)
2) reviewed by the IRB
3) tracked through the review process by Principal Investigators and others
4) modified as necessary to gain IRB approval
5) amended by investigators
6) managed by means of continuing reviews and reports such as those required for adverse events, study deviations, etc.

A step-by-step guide to eProst is available on the home page of the UM Human Subjects Research Office at **http://hsro.miami.edu**. An eProst help desk is available at 305-243-3195.

The following sections define the policies and procedures applicable to the UM eProst system.

eProst User Authentication

eProst uses the University of Miami's CAS (CaneID Authentication System) system to authenticate the identity of users (i.e. to determine that users are who they say they are). CAS is based on the Central Authentication System developed at Yale University. CAS is maintained by the UM Information Technology Office which has implemented the system to require only a single sign-on. This means that users may log into multiple applications with just one username and password.

To ensure security, users must change their passwords at least once every 180 days.

Once a user has successfully logged into the CAS system, CAS passes the user's C-number (a unique identifier, consisting of the letter "C" followed by 8 digits) to eProst. Within eProst, the C-number is matched to an account. By this means, users are allowed to access their personal eProst workspace.

Restricting Access to eProst

Although the CAS system provides *authentication*, it is the eProst system which provides *authorization* to permit a user to access private information in eProst. Access to the eProst system is limited to authorized users and is controlled by authorized HSRO staff members who are responsible for system security.

Persons wishing to access eProst must be approved by the HSRO do to so, which requires completion of an account request form within eProst and acknowledgment of the eProst Use and Confidentiality Agreement. If approved for eProst access, a user shall be given the ***Registered User*** role which allows basic access to the eProst system. By default, most users are also given the ***Protocol Team*** role, which allows the creation, preparation and amending of study applications and related items. Higher levels of access are assigned by the HSRO as needed. These require authorization by the appropriate University or department official, and may require the user to sign a confidentiality agreement. The "level" of authorized access shall be the minimum access necessary for the user to perform required duties and responsibilities; and it will be based on the user's role(s) and responsibilities at the institution and within a particular study.

All study information and documents uploaded into eProst must be regarded as confidential and must not be discussed or disclosed outside of the appropriate functions and/or IRB review process.

If there is a period of 60 minutes of inactivity, a user's session shall be terminated by eProst to prevent unauthorized access to the system.

eProst Account Requests

Unless otherwise approved by the Vice Provost for Human Subject Research, access to eProst is limited to employees, students, fellows or authorized associates of the University of Miami (UM) or Jackson Health System (JHS). Requests for eProst access (i.e. "new accounts") must be submitted online from the eProst web site, using the **New Account Request** form.

When requesting an eProst account, each applicant must agree to comply with the eProst Use and Confidentiality Agreement:

eProst Use and Confidentiality Agreement

I understand that in the course of my employment/assignment with The University of Miami and in the course of performing my work activities, I may come into possession of certain confidential information to be used in conjunction with the Electronic Protocol and Submission Tracking System (eProst).

I understand that such Confidential Information must be maintained in the strictest confidence.

I understand and agree to abide by the terms of the Code of Federal Regulations: Title 21, Chapter 1, Part 11 (21 CFR Part 11), regarding electronic records and electronic signatures. I understand the importance of using my own login to sign on to the eProst system for security reasons, and I understand that my account may not be used by, or reassigned to, anyone else.

I understand that all transactions performed by me will have my user ID associated with the transaction which constitutes an electronic signature, legally equivalent to my handwritten signature. I am responsible for all activities performed under my username and password.

I understand that I am responsible for maintaining the confidentiality of my password and will not give my password to anyone. I will request to have my password changed if I think it might be misused, if it has been shared, or if it has been compromised.

I also understand and agree to abide by the terms of the University's Information Technology policies; including Computer Access and Confidentiality, Use of Computing Facilities, World Wide Web, Use of Electronic Communications, Access Control and User Account Management, and Password Security (policies A045, A046, A047, A053, A130, and A131), which are available to me on the Information Technology Policies and Procedures website (http://www.miami.edu/index.php/it/information_technology_policies_and_procedures/).

Should questions arise in the future about how to protect information to which I have access, I will immediately notify my supervisor or contact the Human Subjects Research Office, 305-243-3195 or eprost@med.miami.edu.

I understand that violation of this agreement may result in disciplinary action up to and including termination and/or legal action.

After verification of the applicant's C-number, status, title, email address, and department/division/center affiliation in DHRS, the eProst account may be created.

Requirements for eProst Accounts

- Each eProst account must be unique to one individual and must not be used by, shared with, or re-assigned to anyone else.
- The account holder is responsible for all activities performed within eProst using that account.
- If an account holder leaves the University of Miami or Jackson Health Systems and later returns to the institution (i.e. UM or JHS), he/she will resume using the same account; a new account will not be created.
- Each eProst user is given a unique username. Once assigned, usernames must not be changed.
- All eProst users must have a CaneID and C-number.

- Every eProst account must be associated with a valid C-number, and each C-number must be associated with only one eProst account.
- A single email address may not be associated with more than one eProst account.

Disabled Accounts

Unless otherwise approved by the Vice Provost for Human Subject Research, accounts will be disabled (1) when an account owner’s affiliation with the University of Miami or Jackson Health Systems ends and the user is no longer involved with any studies approved by the UM IRB, (2) after one year of inactivity (one year from date of last login), or (3) if it is determined that the account has been compromised.

An account that has been disabled due to one year of inactivity may be reactivated upon the request of the user and verification of the user’s current status. A request for reactivation of an eProst account must be submitted via email, from the email address on record in eProst for that account.

Audit Trail

eProst provides a system-generated, time-stamped audit trail (History Log) for all submissions. This “History Log” documents each activity executed within the eProst system, including the identity of the user who executed the activity, date and time of execution, and name of the activity. This history log cannot be altered.

eProst Electronic Signatures

The Human Subjects Research Office considers all electronic approvals executed within the eProst system to be equivalent to handwritten signatures. Users are responsible and accountable for any activities executed using their eProst electronic signatures.

IRB determination letters generated in eProst are not manually signed, because the electronic approval/signature is considered equivalent to a handwritten signature, and there is no regulatory requirement for a handwritten signature. If required by a sponsor and requested by the principal investigator, approval letters may be signed by authorized HSRO staff members.

System Security

The eProst server resides on a secure computer network maintained by the Medical Information Technology Office of the University of Miami, Miller School of Medicine. Non-public information is viewed over SSL (Secure Sockets Layer).

Backup and Recovery Procedures

As a safeguard against accidental data loss, data corruption, vandalism, or hardware failure, eProst data is backed up nightly by an automated process. In the event of accidental deletion or other data loss, the system may be restored from a backup file. The system cannot, however, restore new submissions created or modifications made between the last successful backup and the point in time when the data loss/corruption occurred.

In addition, backup files are created by Medical Information Technology on a nightly basis via IBM's Tivoli tape backup system.

Change Controls

Study and user account data within the eProst system will be backed up prior to any updates to the system, including hardware or software upgrades, hot fixes or patches. All changes to the system configuration are documented in an issue log and patch guide released prior to implementation, and changes are managed in a source control system. Any changes made manually to individual records within the system must be fully documented by the HSRO staff member making or requesting the change.

Training of Personnel

All eProst users are given the opportunity to receive training appropriate to their user role(s) and assigned tasks. Training is conducted when requested to ensure that users are familiar with the system and are kept apprised of system changes that may impact their work. In addition, major system changes are communicated to users via a listserv and the online HSRO newsletter.