Policy and Procedures for PRC Server Privacy and Security

Implementation Date: December 1, 2005
Modification Date: September 2, 2015

Policy

PRC complies with federal laws concerning privacy and security of protected patient health information.

Purpose

To insure that PRC staff maintain HIPAA and CITI compliance.

Procedures

1. A PRC Project Coordinator, or designee, will ensure the authorization and confidentiality of project data.
   a. A signed data use agreement or memorandum of understanding will be on file.
   b. All Protected Health Information (PHI) data will be approved or waived by the UMB Institutional Review Board (IRB) and/or other required institutions.
   c. PRC staff having access to project data will sign a confidentiality form.
   d. Access to the data will be limited to the time period specified in the DUA.

2. The PRC System Administrator (SA) will ensure data security on the server.
   a. The server is contained in a restricted locked room.
   b. All visitors to the system are escorted.
   c. Access to system is granted only if the user is in compliance with HIPAA and CITI training requirements.
   d. Access is only granted to staff, faculty, students, and researchers having current project data maintained on the server.
   e. Accounts are disabled upon unemployment or project termination date.
   f. Accounts are password protected. Three unsuccessful logins results in temporary shut-out of system.
   g. Automatic logoff occurs after 30 minutes of inactivity.
   h. Virus protection is up to date, and software patches are applied in a timely manner.
   i. Original data will be stored in the PRC safe or returned to the PI.

3. All PRC staff will ensure protection of data.
   a. Each member is HIPAA and CITI certified, and understands importance of security measures.
   b. Paper records are stored in locked file cabinets in locked offices and shredded upon completion of the study.
   c. Electronic records are only stored on the secure server and are password protected.
   d. Personal computer screens are obstructed from public sight.

e. User logs off network account and locks door when not in office.
f. No passwords are shared.
g. Any data containing PHI will not be sent via e-mail. Only the file locations may be sent via e-mail. When data must be sent outside PRC, PHI data are scrambled, encrypted and/or de-identified.
h. Remote access requires SOP account, Secure Shell software, firewall, and up-to-date virus protection.
i. Back-up and archive media are stored in PRC on-site and off-site safes.

4. PRC SA provides proper data removal.
   a. PHI data are backed-up regularly onto well-labeled media, and stored in secure locations, both on and off-site.
   b. Following established archival procedures, all data are removed from the system and external media destroyed. The archival procedures are outlined below.
      - All data and program files are zipped and stored on removable media.
      - All data and program files, except SAS programs, are removed from the system.
      - A copy of the archive is saved for a period of 3 years, or a period defined by the contract, whichever is shorter. (In the case of Federal contracts, the time period is dictated by the federally mandated requirements at the time of the contract award or completion, whichever is longer.)
      - A copy of the Contract directory and all documentation is offered to contracting officials.

5. PRC SA provides proper security tracking and termination of system users
   Access to the PRC server follows a set of security standards during initiation. Similarly, security actions are followed to remove individuals to limit access to PRC files, serving as a means for breach of security.
   There are a number of reasons why individuals obtain access to the PRC server system. Students, faculty and staff may request access during the year.
   a. Graduate Program Coordinator will include prc@rx.umaryland.edu in correspondence to assist with initiating server access on a rolling basis.
   b. Graduate Program Coordinator will twice annually, share details of newly enrolling students that may need access to the PRC server.
   c. PRC Systems Administrator will conduct a process of monitoring user access on a rolling basis, tracking login and logout activity by user.
   d. PRC Systems Administrator will compile twice annually an updated list of users who have NEVER or NOT accessed the system in 190 days or more for review by PRC Staff and Graduate Program Coordinator. Once review is completed, names will be recommended for termination from having access to the system.
   e. The list generated twice annually will be used by the Graduate Student Coordinator and PRC staff on a rolling basis to monitor, track and control system granted access and termination accordingly.