Good Research Practice and Data Security Policies
Department of Pharmaceutical and Health Services Research

This policy outlines the Good Research Practices and Data Security Policies for the Department of Pharmaceutical Health Services Research (PHSR) at the University of Maryland, School of Pharmacy. ***ALL faculty, trainees, and staff who conduct research of any kind are required to follow these policies.*** In addition, individuals who utilize the services of Pharmaceutical Research Computing (PRC) are also obligated to follow PRC data security and good research practices, as described below.

Good Research Practices

Good research practices require extensive documentation and implementation of policies to ensure the protection and privacy of human subjects and extant data. Good research practices are mandated at the local, state and federal government levels to ensure the ethical use of human subjects' data. Violations are punishable by monetary fines and in some cases imprisonment.

The study Principal Investigator (PI) has access to research identifiable files (RIF) that contain protected health information (PHI) or personally identifiable information (PII). These individuals therefore ultimately are responsible for maintaining compliance with the data use agreement (DUA) and the Institutional Review Board (IRB) protocol for the study. The University of Maryland Baltimore (UMB) Human Research Protections Office outlines the responsibility of the PI in their Investigator Manual, which is available here: http://www.hrpo.umaryland.edu/policies.asp.

PHSR Department Good Research Practices

Research data generally contain PHI/ PII that could be used to ascertain subject identities and violate subject privacy. For data that contains PHI/PII, good research practices include the elements summarized below.

1. Data access is restricted to: a) personnel with authorized access under approved DUAs, b) project team members named on IRB-approved project protocols that have been approved by through the CICERO system employed by HRPO of UMB.
2. Data are stored securely so that only individuals who are authorized to access the data are able to do so; and
3. The privacy of patient PHI/PII is maintained.

Data Access

This section summarizes the requirements and conditions for data access.

1. All PHSR researchers and their research team members are required to complete HIPAA training and update their CITI certificates biannually as mandated by UMB policies.
2. A copy of the HRPO/IRB approval letter that names all personnel with authorized data access must be on file with PRC before data access will be granted.
3. A current DUA is required.

Note: The PI is responsible for ensuring that requirements 2 and 3 are met. For cross-institutional studies, other IRB requirements also may need to be satisfied. For example, projects with the Veterans

Affairs Maryland Health Care System (VAMHCS) may have additional requirements for obtaining data access.

Data Security

In order to ensure that inadvertent disclosure of PHI/PII does not occur and that only authorized individuals access data, accounts on the secure PRC network are password protected. PRC has a complete Data Management Plan that outlines all security measures. PI's that choose to store their data on PRC's secure system must adhere to all of the measures outlined in that plan.

If an individual chooses not to store their data on PRC's server, the following measures must be followed. More complete details of the Centers for Medicare and Medicaid Services policies can be accessed here: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/DUAs.html.

All faculty, students, trainees, and staff who conduct research of any kind are required to follow University policies. The current UMB IT Computer Work Station Security Policy can be found here: http://www.umaryland.edu/umbcomputingpolicies/it-computer-workstation-security-policy/

Remote access is strictly controlled through the UMB campus authentication and authorization measures. Logon information may not be shared with others. The current UMB IT Remote Access Policy can be found here: http://www.umaryland.edu/umbcomputingpolicies/it-remote-access-policy/

Penalties for Violations of Health Insurance Portability and Accountability Act (HIPAA)

Violation and/or breach of the Health Insurance Portability and Accountability Act (HIPAA) are subject to the civil and criminal penalties detailed below. In addition, the UMB IRB has the authority to temporarily suspend or terminate a study protocol when a breach or HIPAA violation has occurred. Further, ***all*** of the PI's research activities may be terminated, if deemed necessary, to prevent future violations or breach of the HIPAA standards and possible harm to study participants. Repeated violations and/or malicious violations can result in the suspension or termination of a research study and severe violation(s) can result in terminations of all research studies of the offending PI.

Anyone in violation of the HIPAA standards can be faced with civil and/or criminal penalties. The Department of Health and Human Services (DHHS) Secretary determines the punishment based on the extent of the violation and the harm that it caused or had the potential to cause harm. However, civil penalties are not imposed if the violation is corrected within thirty (30) days of occurrence, except in the case of willful neglect. Should the DHHS Secretary determine that criminal activities have occurred; the investigation is transferred to the Department of Justice for further legal action, if warranted. The penalties for violation of HIPAA standards are financially and professionally devastating to the PI. Therefore, staff training is prioritized and there is no tolerance for non-compliance. The DHHS will not accept ignorance of the law as a defense. A description of levels of violations is given below.

1. **Not willful neglect**: If the individual did not know that he/she violated HIPAA and would not have known even if they were reasonably diligent in trying to find out.

2. **Willful neglect corrected**: In cases where HIPAA has been violated because of willful neglect but was corrected within the required thirty (30) days… (For example, when an individual unintentionally sends a fax to an unintended recipient due to careless keying of the fax number.)
3. **Willful neglect not corrected within the specified thirty (30 days)** include the following:
    - **Knowing disclosure of PHI**: Individual knowingly discloses another person's identifiable health information. (For example, an individual discusses a patient's PHI in an elevator, and such conversation is overheard by others.)
    - **False pretense**: Individual knowingly discloses another person's identifiable health information and the violation is made under false pretense.
    - **Malicious disclosure**: Violations committed with the purpose of selling, transferring or using a person's identifiable health information for commercial or personal gain, or to cause malicious harm.

Table 1. Penalties for Violation of the Health Insurance Portability and Accountability Act (HIPAA) Standards

VIOLATION	CIVIL PENALTIES		CRIMINAL PENALTIES
	HIPAA	HITECH	
Reasonable Cause (not willful neglect)[1]	$100 a violation Max: $50,000/yr	$1000 a violation Max: $100,000/yr	NA
Willful Neglect- corrected[2]	$10,000 a violation Max: $50,000/yr	$10,000 a violation Max: $250,000/yr	NA
Willful Neglect-Not corrected[3]	$10,000 a violation Max: $50,000/yr	$50,000 a violation Max: $1,500,000/yr	NA
Knowingly disclose protected data[4]		Up to $50K per occurrence	$50,000 and up to 1-yr imprisonment
Knowingly disclose protected data under false pretense[5]		Up to $100K per occurrence	$100,000 and up to 5-yr imprisonment
Malicious intent to use protected data for personal gain[6]		Up to $250K per occurrence	Up to $250,000 and up to 10-yr imprisonment

https://www.hipaa.com/the-reality-of-hipaa-violations-and-enforcement/
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf

Pharmaceutical Research Computing (PRC) Data Security Policy

The purpose of the PRC Data Security Policy is to provide a uniform standard for ensuring the integrity and security of all of the databases PRC maintains and manages in partnership with the respective clients. PRC aims to assure that high priority and attention is given to maintaining data security to support sound research practices.

The PRC security policy is divided into three main sections: 1) authorization to access PRC servers; 2) access to specific datasets on PRC servers and data storage; and 3) PRC responsibilities to ensure good research practices and reporting of violations. The Authorization section details the necessary steps and documentation that must be provided to PRC to obtain an account that allows access to PRC servers. The Access and Data Storage section describes the determination of access level and required documentation for each access level. The PRC Reporting of Violations section describes PRC's responsibility to ensure sound research practices and data security that is maintained in compliance with local, state and federal guidelines and laws.

AUTHORIZATION

PRC Account Establishment

Access to study data is limited to the PI and IRB-approved study personnel. Authorization for data access and creation of a PRC account follows the procedures noted here.

1. Data access is restricted to personnel named as project team members on project protocols by the PI, approved by the Institutional Review Board (IRB) through the CICERO system employed by HRPO of the University of Maryland, Baltimore (http://www.umaryland.edu/hrp/), and identified under the data use/re-use agreements. It is essential that the role of each study team member be precisely specified in the protocol as this will be used to determine the level of access granted to study team members.
2. All study team members must have completed the required HIPAA and CITI/HRPO human subjects training and have current certificates on file with PRC.
3. All study team personnel are assigned an individual account and a password. Access to the server requires the use of encryption terminal emulation software and server level passwords that are governed by strict rules.
4. Study team members must sign a Confidentiality Form indicating that the person will protect the confidentiality of the data as outlined in the DUA and will not disclose or conduct unauthorized use of the data.
5. Study team members must sign a Data Access Agreement (DAA) indicating that no raw data will be removed, copied, or shared from the PRC system. No PHI data is to be shared via e-mail. Only file locations are sent via e-mail.

PRC maintains this documentation on file for all active projects and requires this documentation prior to establishing an account and for ongoing maintenance of the project space on the PRC server. PRC will review the IRB approval letter and study protocol to determine the level of access for each of the named study team members. The organization employs the principle of least privilege, allowing only authorized users access that is necessary to accomplish assigned tasks.

If study personnel stop working on a project, their access to the data and any derived analytic files is removed. The PI must keep their IRB protocol current with personnel changes. The PI must notify PRC of any staffing changes. PRC tracks project team members' status (active, pending, retired, terminated) and role (Principal Investigator, Analyst, etc.) in their Quality Management Project Plan (QMPP). The PI must notify CMS in an email within thirty (30) days of any project staff changes.

The PRC Systems Administrator monitors data access permissions on a regular basis. PRC personnel review the list of users twice annually, identifies names for removal, and removes system access.

HRPO/IRB Requirements

It is university policy (see http://www.hrpo.umaryland.edu/default.asp) that ALL members of the research team that are to have access to research data be NAMED in the IRB protocol submission. CICERO provides a section that allows the PI to list all study team members and specify their role in the research project. Procedures are in place to allow study team members from other institutions to be vetted with UMB through HRPO/CICERO and will be reviewed on a case by case basis by the PI and PRC director with the guidance of HRPO.

The composition of a study team changes over time, however before new team members will be authorized access to project data on the PRC server, a copy of the IRB modification approval letter must be presented to PRC prior to authorization for new study team members. PRC recognizes this can create unwanted delays in the research program, and will try to help PIs plan in advance in an attempt to minimize delays.

The PI is responsible for ensuring that the IRB is kept current over the course of the study and for as long as the DUA is kept open. A DUA is not valid without an active IRB.

Data Use Agreements (DUA)

In addition to IRB-related documentation, an approved DUA must be submitted to PRC to finalize the AUTHORIZATION process. The DUA will vary depending on the data source(s) used for the research. It is the responsibility of the PI, in collaboration with PRC staff in many cases, to ensure that a valid DUA has been executed and includes signature pages for each individual entering into the DUA agreement. The PI is responsible for ensuring that the DUA is kept current over the course of the study.

Summary of Required Documentation

Documentation required for PRC Systems AUTHORIZATION includes:

- Copy of the full CICERO protocol
- IRB approval letter
- HIPAA form or letter of HIPAA waiver
- Copy of executed DUA
- Completed training certificates (HIPAA & CITI) for all study personnel
- Signed Confidentiality Form indicating that the person will protect the confidentiality of the data as outlined in the DUA and will not disclose or conduct unauthorized use of the data.
- Signed Data Access Agreement that indicates that no raw data will be removed, copied, or shared from the PRC system

- PRC required Systems Training
- For projects that use VA data, the required copy of the VA Research & Development Committee approval letter. A copy of the IRB/VA approved consent form may also be required.

PRC's policies apply to all research identifiable secondary data, including CMS data. PRC forms and policies can be found through this link: http://www.pharmacy.umaryland.edu/centers/prc/policies-and-forms/

Because this authorization process is mandated by university policy, exceptions to this requirement **will not** be made.

ACCESS AND DATA STORAGE

For PIs who choose to store project data on the PRC server, the staff at PRC tracks all DUAs and help manage compliance in a database. This database is an inventory of all DUA's that PRC assists with on the UMB Campus. The tracking database documents: DUA numbers, study titles, receipt dates, expiration dates, custodians, types of data received, destroy dates, dates of disposition completion, and miscellaneous other details. In addition, PRC documents all project related file locations as part of their project task list and management plan. These files are kept current by PRC Project Coordinators.

PRC's Linux server uses Samba and Network File System to provide a data storage area that is seamlessly available to both the PCs and the Linux server. Remote access to the servers is achieved through the use of Secure Shell Protocol (SSH) with PuTTY which provides a secure channel between the client and server.

PRC system users are required to meet with a PRC team member to complete a system training.

Once the proper documentation and training has been reviewed and approved by PRC the study protocol is used to determine which of the three levels of access a study team member is granted as outlined below.

Level 1: View

The most basic level is "view" only whereby the user can see the contents of directories to verify data files and other documents but will not have the capability to open data files or copy/move data around or off the PRC server. This level of access will typically be assigned to study administrators and PIs that are not actively involved in data analyses.

Level 2: Read-Only

The second level of access is "read-only". With this level of access an individual will be able to open data files and run analyses but will not have the capability to create new variables and/or overwrite existing data files. This level of access will typically be provided to analysts that will be responsible for statistical analyses.

Level 3: Read-Write

The third level of access will be "read-write," which designates full access. All PRC staff working on a given project and the PRC leadership will have full access. A limited number of study team personnel will

be granted this level of access to ensure that data integrity is maintained over the course of the study and/or time the data is stored on the PRC servers. Individuals with this level of access will typically be involved in creating data analytic files from the raw-source data and due to this, will almost always need access to PHI, except in the case where data are de-identified. Therefore, it is imperative that this level of access be clearly documented in the IRB/study protocol for these individuals.

Data Storage

PRC has recently upgraded its servers and data security capabilities to better support clients' data security needs. To assure data security and protection of PII/PHI, ALL data files containing PII/PHI are to be stored ONLY on PRC servers. (Note: the one exception is projects with VAHCS where data must be stored and analyzed on VAHCS servers.)

All original media containing data files are kept by PRC in an access-controlled room in a locked safe onsite. Only authorized personnel designated by the PRC Director, have the ability to physically enter the locked office and server room.

The PRC System Administrator is responsible for the upload of data onto the secure servers, which are accessible only to authorized study personnel. The database management at PRC is built with multiple layers of security and follows best practices for securing sensitive data. The main levels of security are fourfold and include: physical security in the offices, data directory access controls, physical server security, and virtual server security. Project computers are all password protected, are protected by the University of Maryland School of Pharmacy (UMSOP) firewall, and are in locked offices within a building with security guard access during office hours and limited, electronic passkey access during off-hours.

PRC follows all UMB campus IT Policies (Work Station and Remote Access). Users of UMB network resources are required to have a user password at startup and must also "Lock Down" (or log out) of the computer each time the computer is left unattended. Individual user sessions must also initiate a password-protected screensaver after a period of no more than thirty (30) minutes of inactivity. Inactivity of a remote (off campus) server session is automatically disconnected after thirty (30) minutes of inactivity. Re-login with password is required for re-entry. The current UMB IT Computer Work Station Security Policy can be found here: http://www.umaryland.edu/umbcomputingpolicies/it-computer-workstation-security-policy/

Remote access is strictly controlled through the same on-campus authentication and authorization measures. Logon information may not be shared with others. The current UMB IT Remote Access Policy can be found here: http://www.umaryland.edu/umbcomputingpolicies/it-remote-access-policy/

PRC strictly enforces log-in/off policies. The security measures in place to track user activity to limit potential breach of security are:

- PRC Systems Administrator will conduct a process of monitoring user access on a rolling basis, tracking login and logout activity of the users as well as user account activity.

- In addition to access being removed on a rolling basis, twice annually, a full system review is conducted and any identified inactive research study team members are removed.
- Users identified by PRC's System Administrator as having sessions of extended duration (e.g. server session lasting longer than eight (8) hours) will be given a warning of their security breach. With each repeated offense, the penalty will become more stringent.
    - ✓ First-time offenders and their Supervisor/Advisor will be notified of the breach. Penalties for second and third breaches will be re-iterated.
    - ✓ Second-time offenders and their Supervisor/Advisor will be notified of the breach and will be locked-out out of the system for a period of two (2) weeks. In addition, the person will be denied remote access to PRC systems.
    - ✓ Third-time offenders and their Supervisor/Advisor will be notified of the breach. The user's access will be restricted to using a PRC provided computer in a room where PRC will monitor the logging in and out. Access will be restricted to Monday through Friday from 9 AM – 5 PM. This quarantine period will be for duration of 6 weeks.

PRC performs system backups that use BitLocker full disk encryption. BitLocker uses 256-bit AES to perform the encryption. Backups are kept onsite in an access-controlled room on campus. As part of PRC's disaster recovery plan, another backup copy is stored at an on-campus offsite location in an access-controlled room. Like PRC's facility, this location is protected by the University of Maryland School of Pharmacy (UMSOP) in a building with a security guard, card access, and limited electronic passkey access during off hours.

If there is a need for portable analytical files, the PI can request that PRC provide a de-identified analytical data set that can be moved outside of the PRC server/network in accordance with the DUA. These instances will be reviewed by PRC in collaboration with the PI on a case-by-case basis upon receiving a written request from the PI. If this request is granted, the PI will be required to sign a waiver absolving PRC of any responsibility for maintaining the security of this data and explicitly acknowledging that the PI will assume total responsibility for the data.

PRC RESPONSIBILITIES TO REPORT VIOLATIONS

Security breaches and other data-related misconduct were specified earlier in this PHSR policy. These serve as a reminder of the importance of data security mandated by local, state, and federal regulations and law. By law and regulation, PRC is required to report any suspected or documented HIPAA violation or breach to the UMB IRB and other regulatory groups (e.g., VA R&D committee).

An information security incident is any event that results in a loss or compromise of data or a loss of the ability to work with those data. Security threats can arise from accidental or intention acts. UMB supports a strong Incident Response Policy. Details and forms associated with this policy can be found here: http://www.umaryland.edu/umbcomputingpolicies/it-incident-response-policy/

When dealing specifically with CMS data, the PI must notify CMS by email immediately after such a breach is suspected wherein the security and privacy of CMS data may have been compromised. Details regarding Federal Incident Response Policies and Forms can be found here: https://www.hhs.gov/ocio/securityprivacy/incidentmanagement/incidentresp.html

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS1253654.html

These policies apply to all research identifiable secondary data, including CMS data.

COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

At the end of the study, PRC staff (a custodian on the DUA) will confirm data to be deleted per the instructions of the PI. The PRC's Systems Administrator will conduct a sweep of the PRC system to assure that all data have been removed and attest to the fact that all raw data files, all analytic files, all backups and the original media in PRC's possession related to the project have been deleted from PRC's production server and/or destroyed through shredding to prevent breach of confidentiality. The CMS certificate of data destruction will be sent to CMS within thirty (30) days of data removal: https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/Downloads/cms10252.pdf