UNIVERSITY of MARYLAND
SCHOOL OF PHARMACY

Pharmaceutical Research Computing
220 Arch Street, 12th floor
Baltimore, MD 21201
prc@rx.umaryland.edu
http://www.pharmacy.umaryland.edu/prc/

Progressive Discipline Policy Regarding PRC's System Security

Approved by the PRC Advisory Board: June 26, 2014
Implementation Date: July 17, 2014
Modification Date: October 1, 2015
Modification Date: October 2018
Modification Date: June 13, 2019

Background

In order to comply with the Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA), federal security requirements outlined by National Institute of Standards and Technology (NIST), and data use agreement (DUA)-required standards, PRC has adopted measures to prevent or minimize compromises to PRC's secure serve such as system security breaches or unnecessary server shutdowns.

Policy

The following policy applies to users identified as compromising PRC's policies and standards as shared through PRC's Annual Security Training. Individuals identified as being in violation of this policy will be given an email warning letter regarding their security breach. Penalties will be applied based on the assessed severity or number of repeated offenses. Penalties could include system restrictions, lockouts, or disabled account access.

Procedures

1. The PRC Director, System Administrator (SA), and Assistant System Administrator (ASA) will consult when a person has been identified not being in compliance with PRC's defined security measures. The severity of the breach will be discussed and an appropriate penalty assessed.

2. A list of people, dates/times, details of their offense, the number of times they have been identified for an infringement, and the mitigation strategy will be collected.

3. First-time offender(s) will be notified along with his/her Supervisor/Advisor of the breach. If the breach is considered as a minor infraction, remediation will include educational counseling as well as details on progressive discipline for subsequent breaches.

4. For second-time offenders, the user and his/her Supervisor/Advisor will be notified by email of the breach and the user will be locked out of the system for 2 weeks. This user will also be denied remote access to PRC systems.

5. For a third offense, the user will be limited 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.

6. Subsequent and ongoing data breaches could lead to a user's revocation of access. User and specifically remote access is a privilege, not an entitlement.