Approved by Chris Urbina, Executive Director and Chief Medical Officer, June 2012

SUMMARY

Individuals who have not been granted access to department sensitive information, email, critical systems and applications, may try to gain access by using software to discover user identification and passwords. Additionally, people may attempt to guess passwords for particular individuals and thus gain unauthorized entry to restricted applications, data and email accounts.

POLICY

To identify potential unauthorized access, intrusion attempts or policy violations, the department will monitor user access and prepare periodic reports for use in making security program adjustments. At a minimum, unsuccessful attempts to log into the department network, department applications with sensitive information or other password-protected documents will be reported to the Office of Information Technology (OIT). After three failed login attempts, the user account attempting access will be disabled and not re-enabled until the user password is reset. This limits the number of attempts hackers or other unauthorized people have to break into department systems.

PROCEDURE

1. Users shall be granted access to department systems and sensitive data as outlined in department Policy 15.17 Access Control.
2. The user account may be disabled and the password reset if more than three failed attempts have been made to gain access. Users who have lost access must contact the department system owner or OIT, in the case of department network access. Refer to department Policy 15.12 Password Management for policies and procedures on reset passwords.
3. OIT shall implement access monitoring for the department network, while program managers shall implement access monitoring for systems containing sensitive information. At a minimum, access monitoring will record failed login attempts and user accounts disabled due to failed access attempts.
4. Any employee not complying with this policy and these procedures may be subject to state personnel system progressive corrective/disciplinary action up to and including termination. Non-employees who do not comply with this policy will be dealt with appropriately.

TOOLS/GUIDANCE/STANDARDS

Policy15.17 Access Control
Policy 15.12 Password Management

REFERENCE

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule §164.308, Administrative Safeguards, (a) (5) (i) (C) Log-in monitoring