Policy: Health Insurance Portability and Accountability Act Security Policy

Board Approved: **9/05**
Revised: 03/10
Reviewed: 11/14, 7/15, 12/15, 02/19

Section: 1.9

The Board is committed to protecting all information systems owned, subscribed to and/or leased by the Board including but limited to hardware, software, storage, network and third party service(s). Board information systems are to be used for Board business purposes in the course of normal operations.

The intent of the Health Insurance Portability and Accountability Act security Policy is to create an environment that maintains the confidentiality , integrity and availability of information for intended users. This is achieved by preventing unauthorized access to information and preventing misuse of, damage to or loss of such information or assets.

The Board will comply with applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA) related to the security of protected health information. The Board's Information Technology Manager administers the Board's risk management process with respect to HIPAA security requirements. The IT Manager insures that a data backup regimen is in place and operational at all times. Procedures related to backup of data are regularly deployed. The Board's Business Continuity Plan includes procedures for maintaining critical board operations in the event of system failure.

The IT Manager periodically conducts, or arranges to have conducted, a risk assessment of the Board's security systems and practices. This Policy and related procedures are updated as necessary in response to environmental or operational changes affecting the security of electronically protected health information. Periodic activity reviews are conducted to identify inappropriate activity and corrective action implemented. All Board applications, whether owned or leased, are protected by virus and malicious software protection.

The Board conducts ongoing security awareness with staff. Topics include, but are not limited to, recognizing and avoiding malicious software, using passwords effectively, and workstation use procedures. Staff are familiar with security and access measures so that only authorized personnel have physical or electronic access to any Board electronic equipment and software applications.

Technical safeguards are employed as necessary to maintain the integrity of data and to insure the security of data during transmission. Once electronic storage media and devices are no longer needed, they are destroyed in a manner that makes recovery of data or use of the device impossible. If the electronic storage media is assigned to another user, specific files deemed to be protected health information (PHI) that are useless to the new user are stored or deleted consistent with the Board's records retention schedule.

System access is granted to staff in a manner consistent with the HIPAA Privacy laws and other state regulations, including specific procedures for access control, password selection, and system use. The Board obtains satisfactory assurance that Business Associates will appropriately safeguard PHI by acquiring appropriate HIPAA Business Association agreements.

The Board regularly monitors electronic information systems for breaches of security. It will mitigate adverse impact of security incidents to the extent practicable, and thoroughly document any security incidents and their outcomes.

Confidentiality of individual information is taken very seriously by the Board. Staff are prohibited from improperly using or disclosing confidential information as detailed in various board policies, particularly the Board Administrative Policy 4.5 "Confidentiality of Person Specific Information". Improper uses include, but are not limited to, curiosity, malicious purpose, or financial gain. Staff are expected to comply with this Policy and related Procedures involving HIPAA mandated security for all electronic devices. Violations of this Policy and/or related procedures will be subject to disciplinary action consistent with Section 6.1 of the Board's Personnel Policy Manual.