

DMH INFORMATION INTEGRITY PROCEDURES

The Department of Mental Health (DMH) Chief Information Officer (CIO) or his/her designee shall determine the need for integrity controls following the result of risk assessment (DMH Policy No. 550.01, Data Security Management Process: Risk Management). The DMH CIO or his/her designee must ensure that general integrity control procedures and integrity checking procedures are implemented to protect Protected Health Information (PHI) and other confidential information from improper alteration and/or destruction.

1. General integrity control procedures:

DMH CIO or his/her designee must:

- a. Ensure that information systems include integrity controls for all hardware and software.
- b. Ensure that all integrity controls are documented in the System Security Documentation defined in DMH Policy No. 554.02, System Access Control Policy: Definitions, and are reviewed and approved by the Departmental Information Security Officer (DISO) or his/her designee.
- c. Ensure that Workforce Members are trained to maintain data integrity.
- d. Examine workflow procedures and system components for reliability and correctness to guard against unauthorized modification or destruction of data.
- e. Protect information systems against environmental threats that would harm data, including air temperature and humidity, fire suppression systems, or weather-related events.
- f. Provide a means for Workforce Members to report suspected unauthorized data modification or destruction in accordance with DMH Policy No. 552.01, Security Incident Report and Response Policy.

2. Integrity checking procedures:

System Managers/Owners must:

- a. Use the integrity controls listed in the Recommended Safeguards Description section of the Risk Management Report of the DMH Policy No. 550.01, Security Management Process: DMH Risk Management.
- b. Determine the directories and files for which data integrity will be checked, including those containing PHI and other confidential information.
- c. Establish a schedule for the checking of stored files in which the frequency of inspection is commensurate with the criticality of each file type, including both

- periodic inspections and event-specific checks (e.g., upon receipt or transmission of information).
- d. Determine the integrity resources and methods that will be used to perform integrity inspections (e.g., cryptographic checksum tools, lists of directories and files and the attributes of each, log files detailing actions taken by users and virus scanners).
 - e. Create baseline reference information based on the integrity control(s) selected (e.g., cryptographic checksums) for the applicable directories and files. The preferred method for recording and accessing the baseline reference data is through a read only medium (e.g., CD-ROM). These records must be stored securely, accessible only to appropriate personnel and protected against environmental threats.
 - f. Check actual directory and file contents and attributes against the baseline reference(s) selected (e.g., cryptographic checksum matching) to determine if there have been any unauthorized (actual or suspected) changes to the system.
 - g. Report any unauthorized (actual or suspected) changes to the system by following DMH Policy 552.01, Security Incident Report and Response Policy.