

PRIVACY AND SECURITY AWARENESS TRAINING PROCEDURE

I. WORKFORCE TRAINING REQUIREMENTS

- A. The privacy and security training must provide Workforce Members with information on how to handle Protected Health Information (PHI) and other confidential information in accordance with the Department of Mental Health (DMH) privacy-related and security-related policies.
1. Health Insurance Portability and Accountability Act of 1986 (HIPAA) Awareness Training (Privacy and Security): This means general privacy and security training for all DMH Workforce Members who have limited or no access to PHI and other confidential information in the course of their work.
 2. HIPAA Comprehensive Training: This refers to role-based privacy training designed for clinical and specialty staff (e.g., psychiatrists, clinicians, interns, and social workers) who have access to PHI and other confidential information or provide direct patient care. This also refers to role-based security training required for System Managers/Owners, System Administrators, and information technology (IT) staff responsible for implementing and maintaining administrative, physical, and technical security safeguards.
 3. HIPAA for Business Associates Training: This refer to the segment of contracted DMH staff who are person(s) or entity that provide certain functions, activities, or services for or to DMH involving that involve the use and/or disclosure of PHI, and such person or entity is not a component of DMH or its workforce.
 4. Security Training Content: DMH security awareness training must include, as a minimum, the following topics:
 - a. Training on guarding against, detecting, and reporting malicious software.
 - b. Rules for creating, changing, and safeguarding passwords.
 - c. Login training, including the importance of monitoring login attempts and reporting discrepancies. Systems will provide previous login information after each successful login.
 - d. Periodic security reminders through automated means, login banners, pamphlets, broadcast e-mails, etc.
 - e. Training on workstation usage and related safeguards. Refer to DMH Policy No. 508.01, Safeguards for Protected Health Information (PHI).
 - f. Security incident reporting.

- g. Training on media control covering removal and receipt of hardware/software including access control, accountability, data backup, data storage, mobile storage devices, and disposal of electronic data.
- h. Training on acceptable use of County information technology resources. Refer to DMH Policy No. 556.01, DMH Acceptable Use For County Information Technology Resources Policy.

The Department of Mental Health Chief Information Officer shall, as appropriate, include additional security awareness training topics aimed at reducing the risk of improper access, use, and disclosure of confidential and/or sensitive information, taking into consideration the information from the System Description Report and the Risk Analysis Report as specified in DMH Policy No. 550.01, Security Management Process: DMH Risk Management.

- B. All members of DMH's workforce must receive both privacy training and security training.
- C. Training for new members of DMH's workforce will include:
 - 1. Training during new employee orientation to address general components for workforce privacy and security compliance. This training includes HIPAA awareness and information that all DMH employees must know related to security and the access, use, and handling of PHI and other confidential information.
 - 2. Training during facility orientation on all policies and procedures regarding PHI privacy and security as they relate to the facility.
 - 3. Job specific orientation to educate employees on confidentiality and to address PHI privacy and the security functions necessary for job performance.
- D. For all members of its workforce whose job responsibilities change because of new or changed policies or procedures, DMH shall update training within 30 days after the effective date of the change.
- E. If an existing employee's job functions change due to a position change within DMH, training on health information privacy and security will be conducted during orientation at the employee's new position, or within the first 30 days after the employee's first work day in the new position, whichever is sooner. (See Section II, "Training Related to Updates or Changes in Policies and Procedures," below.)

II. TRAINING RELATED TO UPDATES OR CHANGES IN POLICIES AND/OR PROCEDURES

Training related to updates or changes in policies and procedures will be executed through workforce training, facility training, or job specific training. Updates and changes will be incorporated into the training materials used for new employee, facility, and job specific orientation.

This training will be an ongoing, evolving process in response to environmental and operational changes affecting the security of electronic information and as DMH's security needs and changes in procedures. The amount and timing of security awareness training will be left to the discretion of the facility but not less than once every two years.

III. TRAINING DOCUMENTATION REQUIREMENTS

- A. Each DMH facility will maintain documentation in electronic or written format on all information security or privacy training provided to members of its workforce.
- B. Documentation of training will consist of date, time, workforce trainee name, and type of training session attended.
- C. Training documentation will be placed in workforce personnel files and/or tracked in a DMH training database.
- D. Training documentation must be retained for six years from the date created or the date when it was last in effect, whichever is later.

If, however, a DMH entity is subject to a longer documentation retention period as a part of a regulatory, compliance, and/or accreditation requirement [e.g., Medicare, Medicaid, Joint Commission on Accreditation of Healthcare Organization (JCAHO)] then the documentation mentioned above must be retained for the longer period.