

WORKFORCE MEMBERS SECURITY PROCEDURES

The Department of Mental Health Chief Information Officer (DMH CIO) or his/her designee must work with System Managers/Owners and the Department of Mental Health Human Resources Bureau (**DMH HRB**) to develop and coordinate implementation of the workforce security procedures.

I. DMH Workforce Authorization and Supervision Procedure

DMH System Managers/Owners must ensure that Workforce Members are granted access authorization in accordance with DMH Policy 551.01, Information Access Management Policy.

The authorization and supervision process must consist of all the following components:

1. DMH Managers/Supervisors must identify and supervise Workforce Members who work with or have access to Protected Health Information (PHI) and other confidential information. DMH Managers/Supervisors must identify the minimum information access required by these Workforce Members to do their job.
2. DMH System Managers/Owners or designees must identify the security levels necessary for securing the system and still allowing Workforce Members to perform their jobs. DMH System Managers/Owners will assign Workforce Members to the minimum-security level that they need to perform their job function.
3. DMH Managers/Supervisors must restrict access to PHI and other confidential information by unauthorized Workforce Members.
4. DMH Managers/Supervisors must provide authorization and supervision to Workforce Members and others who need to be in areas where PHI and other confidential information may be accessed, and take appropriate safeguards to ensure that those who may be exposed to PHI and other confidential information are made aware of the policies protecting that information.

II. DMH Workforce Clearance Procedure

DMH System Managers/Owners must ensure that Workforce Members' access to PHI and other confidential information is limited to the minimum necessary to perform their job responsibilities.

The clearance process must consist of all of the following components:

1. DMH System Managers/Owners or designee must work with DMH HRB to ensure that proper workforce clearance procedures are implemented.
2. DMH System Managers/Owners or designee must ensure that all applications for access to a system are complete and approved by the appropriate workforce Managers/Supervisors. DMH System Managers/Owners must also ensure that each

Workforce Member with access has signed an acknowledgment of the DMH Policy No. 556.01, DMH Acceptable Use For County IT Resources, which defines their responsibility for the protection of the confidentiality, integrity, and availability of all DMH information resources and the restrictions for utilizing those resources.

3. DMH HRB must ensure that each new Workforce Member receives and signs acknowledgment of DMH Policy No. 556.01 during the initial hiring orientation and that each Workforce Member completes the acknowledgment during the annual Performance Evaluation process. Signed acknowledgments will be filed in the Workforce Member's official personnel folder.

III. DMH Workforce Termination Procedure (Access)

DMH System Managers/Owners must ensure that departing Workforce Members' access to all PHI and other confidential information is terminated upon termination of employment.

The termination process must consist of all the following components:

1. The DMH System Manager/Owner must be notified by the Workforce Member's supervisor as soon as possible, but in no circumstance later than the day the Workforce Member's employment or other service arrangement with DMH ends.
2. The DMH System Manager/Owner must terminate the Workforce Member's access to PHI or other confidential information upon notification by the Workforce Member's supervisor when the Workforce Member terminates employment or transfers to another DMH facility or County department. Access termination must be:
 - a. As soon as possible, but in no circumstance later than 5 business days when the end of employment is voluntary.
 - b. As soon as possible, but in no circumstance later than close of the same business day or end of Workforce Member's work shift when the end of employment is involuntary.
3. The Workforce Member's supervisor must notify the DMH System Manager/Owner when a Workforce Member's status/function/responsibility has changed. The System Manager/Owner must promptly review the Workforce Member's access to PHI and other confidential information and must modify the member's access as needed.