



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT SYSTEM PERSON OR ENTITY AUTHENTICATION	POLICY NO. 554.03	EFFECTIVE DATE 04/20/2005	PAGE 1 of 2
APPROVED BY:  Director	SUPERSEDES 500.46 04/20/2005	ORIGINAL ISSUE DATE	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To verify that a person or entity seeking access to Protected Health Information (PHI) and other confidential information is the one claimed.

POLICY

- 2.1 The Department of Mental Health (DMH) must establish and document procedures for each of the following requirements and submit such procedures for approval to the Departmental Information Security Officer (DISO) or designee.
 - 2.1.1 A user authentication mechanism (e.g., unique user identification and password, biometric input, or a user identification smart card) must be used for all Workforce Members seeking access to any network, system, or application that contains Protected Health Information (PHI) and other confidential information.
 - 2.1.2 Two-factor authentication, in which the Workforce Member, in order to obtain remote access, provides two means of identification, one of which is typically physical (e.g., a secure ID card using a one-time code), and the other of which is typically something memorized (e.g., a secret Personal Identification Number, or PIN, which is required for all systems receiving a Risk Analysis Sensitivity score of "High" - see DMH Policy No. 500.29, Security Management Process.)
 - 2.1.3 Workforce Members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and/or Password, smart card, or other authentication information.



**DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE**

SUBJECT SYSTEM PERSON OR ENTITY AUTHENTICATION	POLICY NO. 554.03	EFFECTIVE DATE 04/20/2005	PAGE 2 of 2
--	-----------------------------	-------------------------------------	-----------------------

- 2.1.4 Workforce Members are not permitted to allow other persons or entities to use their unique User ID or password, smart card, or other authentication information.
- 2.1.5 DMH must ensure that Workforce Members make a reasonable effort to verify the identity of the receiving person or entity prior to transmitting PHI and other confidential information.
- 2.1.6 DMH must ensure that person or entity authentication controls implemented under this policy are documented within the System Security Documentation, DMH Policy No. 500.44, System Access Control Policy.

DEFINITION

- 3.1 Authentication: The validation of correctness for both the information itself and the identity of the person who is the author or user of information.

For a more complete definition of terms used in this policy and/or procedure, see the DMH Security Glossary, Attachment I of Policy No. 500.42, Information Technology and Security Policy.

AUTHORITY

MANDATED BY 45 Code of Federal Regulations, Part 164, Subpart C, Section 164.308 (a)(3)(ii) Board of Supervisors Policy Nos.:
 6.100, Information Technology and Security Policy
 6.101, Use of County Information Technology Resources

REVIEW DATE

This policy shall be reviewed on or before January 2010.