Department of Mental Health

TRANSMITTAL LETTER

SUBJECT **Use of Electronic Signatures in Clinical Documentation**		
POLICY NUMBER **DMH 450.1**	**DATE** FEB 0 5 2008	**TL#** 95

Purpose. To establish a DMH policy regarding the use of electronic signatures in clinical record documentation.

Applicability. Applies to all Mental Health Rehabilitation Services (MHRS) providers and to contractors who provide mental health services to DMH community served consumers.

Policy Clearance. Reviewed by affected responsible staff and cleared through appropriate MHA offices.

Implementation Plans. **A plan of action to implement or adhere to this policy must be developed by designated responsible staff. If materials and/or training are required to implement this policy, these requirements must be part of the action plan. Specific staff should be designated to carry out the implementation and program managers are responsible for following through to ensure compliance. Action plans and completion dates should be sent to the appropriate authority. Contracting Officer Technical Representatives (COTRs) must also ensure that contractors are informed of this policy if it is applicable or pertinent to their scope of work. *Implementation of all DMH policies shall begin as soon as possible. Full implementation of this policy shall be completed within sixty (60) days after the date of this policy.***

Policy Dissemination and Filing Instructions. Managers/supervisors of DMH and DMH contractors must ensure that staff are informed of this policy. Each staff person who maintains policy manuals must ensure that this policy is filed in the **DMH** Policy and Procedures Manual, and contractors must ensure that this policy is maintained in accordance with their internal procedures.

ACTION

REMOVE AND DESTROY	**INSERT**
None	DMH Policy 450.1

Stephen T. Baron
Director, DMH

GOVERNMENT OF THE DISTRICT OF COLUMBIA DEPARTMENT OF MENTAL HEALTH	Policy No. 450.1	Date FEB 05 2008	Page 1
	Supersedes: NONE		

Subject: Use of Electronic Signatures in Clinical Documentation

1. **Purpose**. To establish a DMH policy regarding the use of electronic signatures in clinical record documentation.

2. **Applicability**. Applies to all Mental Health Rehabilitation Services (MHRS) providers and to contractors who provide mental health services to DMH community served consumers.

3. **Authority**. Department of Mental Health Establishment Amendment Act of 2001, and MHRS Certification Standards, dated June 17, 2005.

4. **Policy**.

4a. Electronic signatures or computer-generated signature codes are acceptable as authentication of all clinical record content where staff signature is required subject to the guidelines established in Section 5 below.

4b. Providers are not permitted to have consumers electronically sign any documents.

5. **Guidelines**.

5a. In order for a provider to employ electronic signatures or computer-generated signature codes for authentication purposes, the provider shall adopt a policy that permits authentication by electronic signatures or computer-generated signature codes. These provisions can be incorporated into an appropriate existing policy, including, but not limited to, the provider's Clinical Records Policy required under Chapter 34 of Title 22A DCMR. The policy shall be provided to DMH upon request.

5b. At a minimum, the policy governing the use of electronic signatures or computer-generated signature codes shall include adequate safeguards to ensure confidentiality of the codes. Such safeguards include, but are not limited to, the following:

(1) Each user shall:

(a) **Be assigned** a unique identifier that is generated through a confidential access code.

(b) **Certify**, in writing, that he or she will not disclose the unique identifier or confidential access code to anyone and that he or she is the only person authorized to use the electronic signature or computer-generated signature code. This certification shall be provided to DMH upon request.

(2) The provider shall:

(a) **State** in the policy that each identifier shall be kept strictly confidential. The policy shall include a commitment to terminate a user's use of a particular identifier if it is found that the identifier has been misused. "Misused" shall mean that the user has allowed another person or persons to use his or her personally assigned identifier or that the identifier has otherwise been inappropriately used.

(b) **Have** separation from work procedures that ensure that unique identifiers and confidential access codes are de-activated, disabled, or otherwise rendered non-functioning upon the resignation or termination of a user.

(c) **Provide** training, and refresher training as needed, related to use of electronic signatures to current and new employees and maintain documentation of same.

(d) **Monitor** the use of identifiers routinely and take corrective action as needed. The process by which the provider will conduct monitoring shall be described in the policy.

5c. A system employing the use of electronic signatures or computer-generated signature codes for authentication shall include a verification process to ensure that the content of authenticated entries is accurate. The verification process shall include, at a minimum, the following provisions:

(1) The system shall:

(a) **Require** completion of certain designated fields for each type of document before the document may be authenticated, with no blanks, gaps or obvious contradictory statements appearing within those designated fields.

(b) **Require** that correction or supplementation of previously authenticated entries shall be made by additional entries, separately authenticated and made subsequent in time to the original entry. (The original entry cannot be deleted and shall be available for auditing purposes.)

(c) **Make** an opportunity available to the user to verify that the document is accurate and the signature has been properly recorded.

(d) **Be** adequately protected from "Misuse" and free from unauthorized intrusions, by insuring the use of adequate controls, including but not limited to:

i. The system must automatically lock/log off when not in regular use; or
ii. The provider must require authorized users to log off when not regularly using the system.
Log offs shall be timely to prevent any possible intrusions.

(2) The provider shall periodically sample records generated by the system to verify the accuracy and integrity of the system.

Approved By:

Stephen T. Baron
Director, DMH

(Signature) **(Date)**