Department of Behavioral Health

TRANSMITTAL LETTER

SUBJECT Use of Electronic Signatures in Clinical Documentation		
POLICY NUMBER DBH Policy 450.1A	DATE FEB 0 2 2015	TL# 275

Purpose. To set forth a policy regarding the use of electronic signatures in clinical record documentation for the Department of Behavioral Health (DBH).

Applicability. Applies to all DBH-certified providers with a Human Care Agreement, Saint Elizabeths Hospital and MHRS consumers. DBH-certified substance use disorder service providers using DATA as their electronic records system are not required to implement this policy.

Policy Clearance. Reviewed by affected responsible staff and cleared through appropriate Behavioral Health Authority (BHA) offices.

Effective Date. This policy is effective immediately.

Superseded Policy. This policy replaces DMH Policy 450.1, same title, dated January 13, 2015.

Distribution. This policy will be posted on the DBH web site at www.dbh.dc.gov under Policies and Rules. Applicable entities are required to ensure that affected staff is familiar with the contents of this policy.

2/2/2015

Stephen T. Baron
Director, DBH

GOVERNMENT OF THE DISTRICT OF COLUMBIA DEPARTMENT OF BEHAVIORAL HEALTH	Policy No. 450.1A	Date FEB 0 2 2015	Page 1
	Supersedes: DMH Policy 450.1, same title dated January 13, 2015		

Subject: Use of Electronic Signatures in Clinical Documentation

1. **Purpose**. To set forth a policy regarding the use of electronic signatures in clinical record documentation for the Department of Behavioral Health (DBH).

2. **Applicability**. Applies to all DBH-certified providers with a Human Care Agreement, Saint Elizabeths Hospital and MHRS consumers. However, DBH-certified substance use disorder service providers using DATA as their electronic records system are not required to implement this policy.

3. **Authority**. Department of Behavioral Health Establishment Act of 2013 and Mental Health Rehabilitation Services (MHRS) Provider Certification Standards.

4. **Definitions**.

4a. User. For the purpose of this policy, refers to anyone who signs clinical records using the electronic documentation system (e.g., staff and consumers). See section 6b (1).

4b. System integrity. The state of DBH electronic documentation functions performing as intended without being degraded or impaired by changes or disruptions in its internal or external environments. See section 6c (2).

5. **Policy**.

5a. Electronic signatures or computer-generated signature codes are acceptable as authentication of all clinical record content where a staff signature is required, subject to the general guidelines established in Section 6 below.

5b. When a consumer signature for verification of a clinical documentation is needed, providers are required to get an electronic signature. Providers are required to have consumers electronically sign clinical record documentation using an electronic signature pad, a mouse, a finger or a stylus on an electronic web based form.

6. **General Guidelines**.

6a. Providers shall have policies and procedures that require consumer electronic signatures or computer-generated signature codes for authentication purposes.

6b. 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 or agree through the electronic agreement to the use of electronic documentation and signature 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 agreement shall be printed and shall be provided to DBH upon request.

(2) The provider shall:

(a) Have a policy that emphasizes strict confidentiality of each identifier. 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 used inappropriately.

(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 on a routine basis and take corrective action as needed. The process by which the provider will conduct monitoring shall be described in the policy.

6c. 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.

iii. 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, DBH

2/2/2015

(Signature) **(Date)**