

Department of Behavioral Health  
**TRANSMITTAL LETTER**

<b>SUBJECT</b> <b>DBH Privacy Policies and Procedures</b>		
<b>POLICY NUMBER</b> <b>DBH Policy 645.1</b>	<b>DATE</b> JAN 13 2014	<b>TL#</b> 223

**Purpose.** To revise the Department of Behavioral Health (DBH) Privacy Policies and Procedures to include recent changes in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), the District of Columbia Mental Health Information Act (MHIA) of 1978, as amended, the Data-Sharing and Information Coordination Amendment Act of 2010, and 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records. This policy and corresponding DBH Privacy Manual shall be disseminated throughout the Department and made available to Network providers.

**Applicability.** DBH and its participating Network providers (providers that are certified, licensed, or otherwise regulated by DBH and have entered into a contract or agreement with DBH to provide mental health services or supports or alcohol/drug treatment and prevention services).

**Policy Clearance.** Reviewed by responsible staff, including DBH General Counsel and DBH Privacy Officer.

**Implementation Plans.** Specific staff should be designated to carry out the implementation and training as required, and program managers are responsible for following through to ensure compliance.

**Policy Dissemination and Filing Instructions.** Managers/supervisors of DBH and DBH contractors must ensure that staff are informed of this policy and the DBH Privacy Manual. Each staff person who maintains policy manuals must promptly file this policy in the DBH Policy and Procedures Manual, and contractors must ensure that this policy is maintained in accordance with their internal procedures. *A copy of this policy must also be filed in 1000.3 DBH Privacy Manual, located in all programs that use and disclose PHI (See Section 14 of the policy).*

**ACTION**

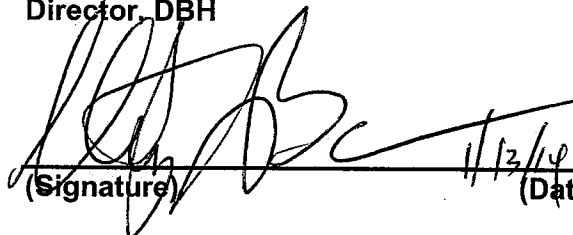
**REMOVE AND DESTROY**


**DMH Policy 645.1, dated July 16, 2003, and  
DMH Privacy Policies and Procedures Manual,  
1000.3, dated July 16, 2003**

**INSERT**

**See Filing Instructions Above**

**Stephen T. Baron  
Director, DBH**

  
(Signature) 1/13/14 (Date)

GOVERNMENT OF THE DISTRICT OF COLUMBIA  <b>DEPARTMENT OF BEHAVIORAL HEALTH</b>	<b>Policy No.</b> 645.1	<b>Date</b> JAN 15 2014	<b>Page 1</b>
<b>Supersedes</b> DMH Policy 645.1, DMH Privacy Policies and Procedures, dated July 16, 2003			
<b>Subject: DBH Privacy Policies and Procedures</b>			

1. **Purpose.** To implement guidelines and procedures consistent with federal and District law that protect the privacy of consumers' health information. The governing privacy guidelines are described in this policy. Specific topics and procedures are addressed in 1000.3, Department of Behavioral Health (DBH) Privacy Manual.
2. **Applicability.** DBH and its participating Network providers (providers that are certified, licensed, or otherwise regulated by DBH and have entered into a contract or agreement with DBH to provide mental health services or supports or alcohol/drug treatment and prevention services).
3. **Authority.** Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and its implementing regulations at 45 Code of Federal Regulations Parts 160 and 164, and the District of Columbia Mental Health Information Act (MHIA) of 1978, as amended (D.C. Official Code §7-1201.01 *et seq.*), the Data-Sharing and Information Coordination Amendment Act of 2010, and 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records.
4. **Definitions.** For purposes of this policy and the DBH Privacy Manual:
  - 4a. **Network Providers** – providers that are certified, licensed, or otherwise regulated by DBH and have entered into a contract or agreement with DBH to provide mental health services or supports or alcohol/drug treatment and prevention services.
  - 4b. **Protected health information (PHI)** - any written, recorded, electronic (ePHI), or oral information which either (1) identifies, or could be used to identify, a consumer; or (2) relates to the physical or mental health or condition of a consumer, provision of health care to a consumer, or payment for health care provided to a consumer. PHI does not include information in the records listed in subsection (2) 45 C.F.R. § 160.103.
  - 4c. **Workforce members** - every employee in the DBH Network. Workforce members include public and private employees and contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
  - 4d. **Covered entity** - (1) a health plan; (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the DBH Privacy Manual. DBH and participating network providers who transmit health information electronically are covered entities. Covered entity shall also include the designated health care components of the District government's hybrid entity or a District agency following HIPAA best practices.
  - 4e. **Consumer** – For purposes of this policy and DBH Privacy Manual, A person who seeks or receives behavioral health services funded or regulated by DBH.
5. **Policy.**
  - 5a. It is the policy of DBH to protect the privacy of consumers' health information that DBH and its participating network providers create, receive or maintain in their respective roles as health care providers.

5b. Each Network provider must ensure compliance with the DBH Privacy Manual, HIPAA, MHIA, Data-Sharing and Information Coordination Amendment Act of 2010, and 42 CFR Part 2 as applicable, pursuant to this policy and its own legal obligations.

5c. Each workforce member with access to PHI must, at all times, comply with the policies and procedures set out in the DBH Privacy Manual.

5d. Workforce members shall consult with their Privacy Officer or designee before they use or disclose PHI if there is any doubt regarding whether such use or disclosure is permitted by the DBH Privacy Manual.

5e. Failure to comply with the DBH Privacy Manual may subject DBH employees to discipline in accordance with Chapter 16 of the District Personnel Manual and applicable collective bargaining agreements, and all workforce members to potential civil and criminal penalties.

5f. Network providers must inform the DBH Privacy Officer of any complaints regarding the use or disclosure of a consumer's PHI.

## **6. Privacy Officers.**

6a. The DBH Privacy Officer in cooperation with the District-wide Privacy and Security Official is responsible for developing, maintaining, and implementing the DBH Privacy Manual, and for overseeing DBH compliance with HIPAA, MHIA, Data-Sharing and Information Coordination Amendment Act of 2010, 42 CFR Part 2, and other applicable federal and state privacy laws.

6b. The DBH Privacy Officer shall serve as the Privacy Officer for the Behavioral Health Authority offices and programs, and as the senior Privacy Officer for the Department, may appoint subordinate privacy officers as needed.

6c. Network providers shall designate personnel and establish systems to carry out the duties of a Privacy Officer as required by HIPAA and the DBH Privacy Manual.

## **7. Workforce Training.**

7a. Each workforce member who may have access to or use of PHI shall receive training on the DBH Privacy Manual as necessary and appropriate for the member to carry out his or her job functions. Network providers must maintain a record of the workforce members trained in accordance with HIPAA.

7b. The DBH Privacy Officer shall work with the DBH Training Institute and the DBH Division of Human Resources (for new employee orientation) to facilitate training DBH employees, including determining the appropriate training content needed by particular trainees and new hires to carry out their job functions.

7c. DBH workforce members will receive privacy training during New Employee Orientation, and shall sign the Form 15, Confidentiality and Security of PHI, to be filed in the employee's personnel folder. Mandatory annual compliance training shall include review of HIPAA, MHIA, the Data-Sharing and Information Coordination Amendment Act of 2010, and 42 CFR Part 2 requirements.

## **8. Workforce Sanctions.**

8a. DBH workforce members who violate the DBH Privacy Manual, HIPAA, MHIA, Data-Sharing and Information Coordination Amendment Act of 2010, 42 CFR Part 2 or other applicable federal or state privacy laws shall be subject to discipline in accordance with Chapter 16 of the DPM and applicable collective bargaining agreements.

8b. Network providers must have sanctions in place for workforce members who violate the DBH Privacy Manual, HIPAA, MHIA, Data-Sharing and Information Coordination Amendment Act, or 42 CFR Part 2 if applicable.

8c. All workforce members (including DBH employees) may face civil and criminal penalties for violation of the MHIA, HIPAA, the Data-Sharing and Information Coordination Amendment Act or 42 CFR Part 2 if applicable.

9. **Reporting Workforce Privacy Violations.** Each workforce member is obligated to report promptly any suspected violation of the DBH Privacy Manual, HIPAA, MHIA, Data-Sharing and Information Coordination Amendment Act of 2010, 42 CFR Part 2, or other applicable federal or state privacy laws to their Privacy Officer or the District-wide Privacy and Security Official. Reports may be made anonymously. In addition, workforce members and consumers may file HIPAA complaints with U.S. Department of Health and Human Services (HHS).

Each workforce member must cooperate fully with any investigation, corrective action or sanction instituted by their Privacy Officer. This includes providing information to authorized representatives of the DBH if an investigation relates to an official matter and the information is obtained during the course of employment or as a result of relationships incidental to employment and the furnishing of a signed sworn or affirmed statement. Failure to cooperate with an investigation may constitute the basis for disciplinary action, up to and including termination of employment or termination of an existing contractual relationship, subject to all employee rights under any applicable collective bargaining agreement and the District Personnel Manual.

10. **Mitigation.** Network providers shall initiate corrective action whenever an improper use or disclosure of PHI occurs by one of their workforce members or business associates.

11. **Retaliatory Acts.** Network providers shall not tolerate any workforce member who attempts to intimidate, threaten, coerce, discriminate or retaliate against an individual who:

- Exercises any right, including filing complaints, under the DBH Privacy Manual or other privacy laws.
- Complains to, testifies for, assists or participates in an investigation, compliance review, proceeding or hearing by a governmental authority.
- Opposes any act or practice that violates HIPAA.

12. **Document and Record Retention.** Network providers must ensure that all documentation required by the DBH Privacy Manual is maintained at least six (6) years after the later of its creation or last effective date, and in accordance with each agency's document retention schedule.

13. **Data Privacy Protection.** Network providers shall implement and comply with reasonable and appropriate administrative, physical, and technical safeguards to secure the privacy of PHI against any intentional or unintentional use or disclosure in violation of the DBH Privacy Manual or HIPAA. (See Part VII of the DBH Privacy Manual for security policies and procedures).

14. **Distribution/Location of the Manual.** The DBH Privacy Manual 1000.3 shall be available on the DBH website. DBH Managers and Network providers shall ensure that a copy of the manual is provided to all of their programs that require its use. It shall be placed in a prominent location where it is accessible to all employees that use and/or disclose PHI.

Approved By:

Stephen T. Baron  
Director, DBH

(Signature)

1/13/14  
(Date)