Department of Mental Health
TRANSMITTAL LETTER

SUBJECT Revised DMH-HIPAA Form 15, dated 12/20/11		
POLICY NUMBER DMH Policy 645.1	DATE JAN 0 9 2012	TL# 157

Purpose. To transmit a revised DMH-HIPAA Form 15, Confidentiality and Security of Protected Health Information (PHI). The form was generally updated to include Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Mental Health Information Act (MHIA) violations and penalties.

Applicability. Department of Mental Health (DMH) and its participating Network providers.

- *Network* means an organized health care arrangement consisting of DMH, and every mental health provider that is certified, licensed, or otherwise regulated by DMH, or has entered into a contract or agreement with DMH for the provision of mental health services or mental health supports.

*EFFECT*IVE IMMEDIATELY:

DMH and its participating Network providers shall use the revised DMH-HIPAA Form 15, Confidentiality and Security of Protected Health Information, dated 12/20/11 (attached).

New DMH employees must complete DMH-HIPAA Form 15, Confidentiality and Security of Protected Health Information, during new employee orientation and current DMH employees who have not completed the form must complete DMH-HIPAA Form 15 during the annual DMH Mandatory Compliance Training.

Participating Network providers must develop internal procedures to ensure employees complete DMH-HIPAA Form 15.

Policy Clearance. Reviewed by affected responsible staff, including DMH General Counsel, and DMH Privacy Officer.

Implementation Plans. A plan of action to implement or adhere to this transmittal must be developed by designated responsible staff. If materials and/or training are required to implement this transmittal, 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. *This transmittal is effective immediately.*

Policy Dissemination and Filing Instructions. Managers/supervisors of DMH and DMH contractors must ensure that staff are informed of this transmittal. Each staff person who maintains policy manuals must promptly file this transmittal with their **DMH** Policy and Procedures, and contractors must ensure that this transmittal is maintained in accordance with their internal procedures. *A copy of this transmittal must also remain in the Privacy Policies and Procedures Operations Manual, which must be located in all programs that use and disclose protected health information (PHI).*

ACTION

REMOVE AND DESTROY
DMH-HIPAA Form 15, dated 6/03

INSERT
This transmittal and the attached revised DMH-HIPAA Form 15, dated 12/20/11 in the DMH Privacy Policies and Procedures Manual dated July 16, 2003.

1/9/12

Stephen T. Baron
Director, DMH

CONFIDENTIALITY AND SECURITY OF PROTECTED HEALTH INFORMATION

Protected health information (PHI) means any written, recorded, 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. Laws governing the confidentiality and security of PHI include HIPAA (Health Insurance Portability and Accountability Act of 1996) under federal law and the MHIA (Mental Health Information Act of 1978 as amended) under District law.

District of Columbia and federal laws require that PHI of all present and former consumers be kept confidential, subject to specific allowable uses and disclosures, and that PHI be appropriately safeguarded from unauthorized access.

I understand that mental health information is subject to greater restrictions than general health information in accordance with the MHIA.

I understand that I hold a position of trust relative to PHI owned and/or maintained by the District of Columbia in all formats and computer systems and I have a responsibility to preserve the confidentiality and security of such information.

Accordingly, I understand that I am prohibited from engaging in inappropriate conduct, which may include, but is not limited to, the types of actions listed below:

- Release of any PHI without the appropriate authorization, unless the release is specifically allowed under District or federal law.
- Inappropriate discussion or display of PHI in public areas.
- Failing to safeguard physical locations where PHI is available.
- Failing to safeguard PHI that is carried or maintained in my possession.
- Knowingly gaining, attempting to gain, causing access to, or permitting unauthorized use of or disclosure of any PHI owned and/or maintained by the District of Columbia in all formats and computer systems.
- Using, attempting to use, causing or permitting the use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems for personal gain or motive.
- Knowingly including or causing to be included any false, inaccurate, or misleading entry into any publicly funded computer system.
- Removing or causing to be removed, without proper reason and authorization, any necessary and required information owned and/or maintained by the District of Columbia in all formats and computer systems.
- Abiding, abetting, or acting in conspiracy with another to violate this agreement.
- Divulging my access codes to anyone.

I agree to adhere to the DMH Privacy Policies and Procedures regarding the protection of PHI. Any unauthorized or inappropriate use of PHI owned and/or maintained by the District of Columbia in all formats and computer systems, by the user or by another who has inappropriately been permitted or enabled access to the system by the user, may subject the user to criminal and civil sanctions pursuant to federal and state law as well as disciplinary action up to and including removal.

- MHIA violations can lead to civil penalties for damages and costs, and criminal penalties to include a fine of up to $4,000 and up to 90 days in jail.
- HIPAA violations can lead to civil penalties to include a fine up to $50,000 or more per violation with a calendar year cap of $1,500,000, and criminal penalties to include a fine up to $250,000 and up to 10 years in jail.

I acknowledge that I have received a signed copy of this document.

Name of Employee (print) _____ **Program/Organization** _____

Signature of Employee _____ **Date** _____

Questions related to this form or PHI may be directed to the DMH Privacy Officer.