Department of Mental Health

TRANSMITTAL LETTER

SUBJECT **Wireless Communication Devices and Other Portable Technology Equipment**		
POLICY NUMBER **811.1C**	DATE JAN 1 0 2013	TL# 182

Purpose. To generally update the policy and address the protection of protected health information (PHI) on wireless communication devices and other portable technology equipment.

Applicability. Department of Mental Health (DMH) employees (including interns and residents and contracted medical professionals). Also see Section 9 of the policy regarding Mental Health Rehabilitation Services (MHRS) Providers and contractors.

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. Enforcement will be applicable to current requests for wireless communication devices and other portable technology equipment.***

Policy Dissemination and Filing Instructions. Managers/supervisors of DMH 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
DMH Policy 811.1B, Wireless Communication Devices and Other Portable Technology, dated 10/19/2009	DMH Policy 811.1C, Wireless Communication Devices and Other Portable Technology Equipment

1/10/13

Stephen T. Baron
Director, DMH

GOVERNMENT OF THE DISTRICT OF COLUMBIA DEPARTMENT OF MENTAL HEALTH	Policy No. 811.1C	Date JAN 1 0 2013	Page 1
	Supersedes 811.1B Wireless Communication Devices and Other Portable Technology, dated 10/19/2009		

Subject: Wireless Communication Devices and Other Portable Technology Equipment

1. **Purpose**. To establish the criteria for issuance, use, and maintenance of wireless communication devices and other portable technology equipment (as defined in Section 5d below), in compliance with federal and District privacy laws and regulations.

2. **Applicability**. Department of Mental Health (DMH) employees (including interns and residents and contracted medical professionals). Also see Section 9 regarding Mental Health Rehabilitation Services (MHRS) Providers and contractors.

3. **Authority**. Department of Mental Health Establishment Amendment Act of 2001, and Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA).

4. **Policy**. DMH will support maximum productivity and cost-effectiveness when employing wireless communication devices and other portable technology equipment in service delivery and effectively managing the usage of these devices by employees, while ensuring protected health information (PHI) is secured.

5. **Definitions**.

5a. Secure Network Drives – For purposes of this policy, secure network drives include the employee's personal drive (H) drive, or a program or office shared drive (S). The Global Drive is not considered a secure Network Drive. PHI should never be stored on the Global (W) drive, which has unlimited access, unless in a restricted folder.

5b. Protected Health Information (PHI) - 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 the federal Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA) and the District Mental Health Information Act of 1978 as amended (MHIA).

5c. Sensitive Information – Any confidential information such as PHI, privileged information under attorney/client relationship, information related to privacy act, or proprietary information.

5d. Wireless communication devices and other portable technology equipment - A device that transmits and receives data, text, and/or voice without being physically connected to a network. This definition includes but is not limited to such devices as cellular telephones, laptops, flash drives, pagers, wireless internet services, wireless data devices (e.g., blackberry devices), wireless air cards, and cellular telephone/two-way radio combination devices and satellite phones.

5e. Encrypted – The reversible conversion of readable information into unreadable, protected form so that only a recipient who has the appropriate "key" can convert the information back into original readable form.

5f. Virtual Private Network (VPN) - VPN extends a private network and the resources contained in the network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network. This is done by establishing a virtual point to point connection through the use of dedicated connections, encryption, or a combination of the two.

6. **Procedures and Responsibilities**.

6a. **Employee qualifications to receive portable communication devices**. The employee shall meet one or more of the following criteria in order for a wireless communication device to be assigned:

(1) The duties of the position or assignments are such that immediate emergency response is critical to successfully carrying out the job;

(2) The duties of the position or assignments require response and decision-making to life threatening or other safety issues and situations;

(3) The duties or assignments associated with the position make it necessary that the incumbent be accessible to communicate with senior management or job-related stakeholders at any time;

(4) The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool; or

(5) The duties of the position may lead to potentially dangerous scenarios and situations and there is no acceptable and reliable alternative communication system.

6b. **The Employee** shall:

(1) Store PHI on Secure Network Drives. In the exceptional circumstances that PHI cannot be immediately stored on Secure Network Drives, PHI may be stored on government issued wireless communication devices only if the device is encrypted and/or password protected by DMH. This includes, but is not limited to email and laptops.

(a) USB (flash drives) may not be used to store PHI. Exceptions may be granted by the Chief Information Officer/designee only on a case by case basis.

(b) Employees must be able to account for which consumer's PHI is contained on the portable device in the event that a portable device is lost /stolen.

(2) Follow the chain of command for approval when requesting a wireless communication device and other portable technology equipment with appropriate justification depending on job requirements (see Exhibit 1, Request Form for Wireless Communication Device and Other Portable Technology Equipment):

(a) Supervisor
(b) Program Manager/Department Head

(c) DMH Chief Information Officer/designee

(3) Be responsible for the proper use and protection of property coming into his/her custody and control, and take reasonable precautions to secure equipment appropriately.

(4) Understand that portable communication devices are for business purposes only.

(5) Complete and sign the Record of Acknowledgement of Receipt of Wireless Communication Device (Exhibit 2), and provide form to DMH Information Services.

(6) Not use the portable device while driving.

(7) Not access or transmit sexually explicit material (including pornography), fraudulent information, harassing material, or racially derogatory information.

(8) Not store any data on the equipment that is not business-related (e.g. music, video, etc.).

(9) Not access PHI from any personal wireless communication device unless using VPN technology.

(10) Take reasonable measures to prevent the inadvertent communication of sensitive information to the wrong person.

(11) Report inoperable or damaged portable communication device to his/her supervisor and DMH Information Services within twenty four (24) hours upon discovery.

(12) Report lost, missing, stolen, portable communication device to his/her supervisor and DMH Information Services at DMHIT@dc.gov immediately, and within twenty four (24) hours or the next business day upon discovery, complete a Major Unusual Incident report, in accordance with DMH Policy 480.1C, Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs).

(13) Return wireless communication device and other portable technology equipment to DMH Information Services upon separation from DMH, or when the qualifications stated in Section 6a above are no longer applicable.

6c. **The Supervisor** shall:

(1) Review employee's requests per requirements of his/her position description and job assignments.

(2) Ensure that use of device or equipment is for approved reasons and in compliance with this policy and all applicable federal and District laws, rules, and regulations. Any improper use of DMH issued wireless devices may result in employee disciplinary action up to and including termination.

(3) Be responsible for controlling and managing wireless devices and related services. Ensure that no employee is permitted to exchange, upgrade, or substitute his/her wireless communication device without approval of DMH Information Services. A wireless device is only to be used by the individual to whom it is issued.

(4) Ensure that employees are aware of the dangers associated with driving while using wireless devices, particularly while driving a government vehicle.

(5) Closely manage allocation of wireless communication devices to employees. This includes assessing an employee's use both prior to ordering a new device and periodically thereafter; and contacting DMH Information Services prior to an employee's separation/transfer to confirm what portable devices have been issued to the employee and ensure devices are returned.

(6) Follow employee separation procedures, including notification of the Division of Human Resources, financial officer, and DMH Information Services when an employee is separating from DMH (see DMH Policy 770.1A Clearance of Personnel for Separation or Transfer).

(7) Ensure that the employees who no longer meet the qualifications stated in Section 6a above return the portable device to DMH Information Services.

6d. **The Chief Information Officer/designee** shall:

(1) Be responsible for procurement, installation, selection of equipment and peripherals in accordance with the DC Office of the Chief Technology Office (OCTO) and DMH standards and inventory control.

(2) Maintain tracking records whenever property is distributed to individuals or returned. Also see Section 6b(5) above.

(3) Provide support and maintenance for portable devices and peripherals.

(4) Communicate to users that when using these devices/equipment, security can be compromised. Employees are to use caution and good judgment when communicating sensitive information via wireless devices.

(5) Ensure an Information Services staff member works with the user to ensure the device is properly secured via encryption and/or password protected prior to final distribution to the user.

(6) Ensure that established protocols are followed and documented accordingly in the case of lost, missing, or stolen wireless devices.

(7) Provide final approval of requests for portable communication devices/peripherals in accordance with Section 6a above, which includes justification and recommendation of employee's supervisor. Provision of portable communication devices/peripherals is contingent upon availability of DMH resources.

7. **Consequences for Unauthorized Use of Wireless Communication Devices and Other Portable Technology Equipment**.

7a. The unauthorized use of wireless communication devices and other portable technology equipment is prohibited. Violations may result in removal of assigned equipment, reimbursement by DMH employee for replacement, and/or disciplinary action including termination (see District Personnel Manual, Chapter 16 for guidelines).

7b. 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 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.

8. **Reimbursement**. DMH reserves the right to recoup the value of any unreturned, damaged, or lost property that was loaned to a DMH employee through all appropriate means on a case by case basis, including from the employee's final pay check.

9. **Specific Guidance for MHRS Providers and contractors**.

9a. MHRS providers and contractors who have an agreement with DMH to provide mental health services and supports shall have policies and procedures in place to:

- Ensure the confidentiality and security of PHI owned and/or maintained by the District of Columbia in all formats and computer systems in accordance with HIPAA and the MHIA.
- Prohibit storing any PHI on wireless communication devices unless the device is encrypted and/or password protected to ensure that PHI is appropriately safeguarded from unauthorized access.

9b. Failure to ensure compliance with HIPAA and MHIA may result in consequences pursuant to the provider's contract with DMH, in addition to federal and District civil and criminal actions.

9c. The DMH Office of Accountability will monitor MHRS providers during routine reviews to ensure policies are in place regarding the protection of PHI on wireless communication devices as stated above.

10. **Training**. The DMH Information Services will provide training on this policy to DMH employees who receive portable communication devices.

11. **Related References**.

DMH Policy 623.1 Accountability for Government Property
DMH Policy 480.1C Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs)
DMH Policy 770.1A Clearance of Personnel for Separation or Transfer
DMH Policy 645.1, DMH Privacy Policies and Procedures
District of Columbia Mental Health Information Act of 1978, as amended (MHIA)
Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA)
Health Information Technology for Economic and Clinical Health Act (HITECH)

12. **Exhibits**.

Exhibit 1 – Request Form for Wireless Communication Device & Other Portable Technology
Exhibit 2 – Record of Acknowledgement of Receipt of Wireless Communication Device

Approved by:

Stephen T. Baron
Director, DMH

1/10/13

(Signature) **(Date)**

REQUEST FORM FOR WIRELESS COMMUNICATION DEVICE AND OTHER PORTABLE TECHNOLOGY EQUIPMENT

Instructions: Follow the chain of command for approval when requesting wireless communication device and other portable technology equipment with appropriate justification depending on job requirements:

Requested by: _____ Date: _____
Employee Name and Title

Type of Device Requested (Wireless communication device and other portable technology equipment - A device that transmits and receives data, text, and/or voice without being physically connected to a network. This definition includes but is not limited to such devices as cellular telephones, laptops, flash drives, pagers, wireless internet services, wireless data devices (e.g., blackberry devices), wireless air cards, and cellular telephone/two-way radio combination devices and satellite phones.

Justification (Check all that apply):

Employee qualifications to receive portable communication devices. The employee shall meet one or more of the following criteria in order for a wireless communication device to be assigned.

( ) The duties of the position or assignments are such that immediate emergency response is critical to successfully carrying out the job;

( ) The duties of the position or assignments require response and decision-making to life threatening or other safety issues and situations;

( ) The duties or assignments associated with the position make it necessary that the incumbent be accessible to communicate with senior management or job-related stakeholders at any time;

( ) The duties of the position require a significant amount of travel during regular work hours, making the wireless device a productivity enhancement tool; or

( ) The duties of the position may lead to potentially dangerous scenarios and situations, and there is no acceptable and reliable alternative communication system.

Approvals	Signature	Date
Supervisor		
Program Manager/Department Head		
DMH Chief Information Officer/designee		

RECORD OF ACKNOWLEDGEMENT OF RECEIPT OF WIRELESS COMMUNICATION DEVICE

Property issued to: Name:_____ (Last) (First) (MI)	AGENCY	OFFICE/DIVISION	LOCATION/BLDG.

I have received the item(s) listed below on: (insert date of receipt) _____. **I understand and will abide with the following per DMH Policy 811.1C, Wireless Communication Devices and Other Portable Technology Equipment:**

(1) I will store PHI on Secure Network Drives. In the exceptional circumstances that PHI cannot be immediately stored on Secure Network Drives, I will store PHI on government issued wireless communication devices only if the device is encrypted and/or password protected by DMH. This includes, but is not limited to email and laptops. I will not store PHI on USB (flash drives). I understand that any exception must be granted by the Chief Information Officer/designee on a case by case basis.

(2) I will be responsible for the proper use and protection of this property, and will take reasonable precautions to secure equipment appropriately.

(3) I understand that this property is for business purposes only.

(4) I will not use the portable device while driving.

(5) I will not access or transmit sexually explicit material (including pornography), fraudulent information, harassing material, or racially derogatory information.

(6) I will not store any data on the equipment that is not business-related (e.g., music, video, etc.).

(7) I will not access PHI from any personal wireless communication device unless using VPN technology.

(8) I will take reasonable measures to prevent the inadvertent communication of sensitive information to the wrong person.

(9) I will report inoperable or damaged portable communication device to my supervisor and DMH Information Services within twenty four (24) hours upon discovery.

(10) I will report lost, missing, stolen, portable communication device to my supervisor and DMH Information Services at DMHIT@dc.gov immediately, and within twenty four (24) hours or the next business day upon discovery, complete a Major Unusual Incident report in accordance with DMH Policy 480.1C, Reporting Major Unusual Incidents (MUIs) and Unusual Incidents (UIs).

(11) I will return wireless communication device and other portable technology equipment to DMH Information Services upon separation from DMH, or when my job assignments no longer qualify me to have this device per Section 6a of DMH Policy 811.1C.

The unauthorized use of wireless communication device and other portable technology equipment is prohibited. Violations may result in removal of assigned equipment, reimbursement by employee for replacement, and/or disciplinary action including termination (see District Personnel Manual, Chapter 16 for guidelines).

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 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.

Reimbursement. DMH reserves the right to recoup the value of any unreturned, damaged, or lost property that was loaned to a DMH employee through all appropriate means on a case by case basis, including from the employee's final pay check.

Item No.	Description			
	Description	Model	Serial #	Accessories

Signature of Recipient: _____ Date : _____

Signature of Issuer: _____ Date: _____

Printed Name and Title of Issuer: _____